PLANET
Networking & Communication

User's Manual

2.4GHz 802.11n Wireless Outdoor Access Point

► WNAP-6306

www.PLANET.com.tw

Copyright

Copyright © 2012 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance, (example-use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions:

(1) This device may not cause harmful interference

(2) This Device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Energy Saving Note of the Device

This power required device does not support Standby mode operation.

For energy saving, please remove the DC-plug to disconnect the device from the power circuit. Without remove the DC-plug, the device still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to remove the DC-plug for the device if this device is not intended to be active.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: except the channel 10 through 13, law prohibits the use of other channels.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET 802.11n Wireless Outdoor Access Point

Model: WNAP-6306

Rev: 1.0 (April, 2012)

Table of Contents

Chapter 1. Product Introduction **9**

1.1 Package contents **9**
1.2 Product Description **9**
1.3 Product Features **12**
1.4 Product Specification **13**
1.5 Wireless Performance **15**

Chapter 2. Hardware Description **16**

2.1 LED Panel **16**
2.2 LED Indications **16**
2.3 Port & Connector **17**
2.4 PoE Injector **18**

Chapter 3. Hardware installation **19**

3.1 Preparation before Installation **19**
3.1.1 Professional Installation Required 19
3.1.2 Safety Precautions 19
3.1.3 Installation Precautions 19
3.2 Hardware Installation **22**
3.2.1 Connect Up 22

Chapter 4. Software Installation **24**

4.1 Software Configuration **24**
4.2 Connecting the AP **24**
4.3 Web Login **28**

Chapter 5. Basic System Settings **30**

5.1 System Information **30**
5.1.1 System 30
5.1.2 LAN Info 30
5.1.3 Wireless Info 30
5.1.4 Secondary AP 31
5.1.5 Statistics 32
5.2 System Log **32**
5.3 Internet Setup **33**
5.3.1 WISP 33
5.3.2 WAN Type 34
5.4 Wireless Management **37**

5.4.1 Wireless Setup 37
5.4.2 Multiple AP Setup 48
5.5 Wireless LED Thresholds 49
5.6 LAN Setup 50
5.6.1 LAN IP Address 50
5.6.2 DHCP Server 51
5.6.3 DHCP Client Info 52
5.7 Application & Game - UPnP 52
5.8 Routing 52
5.9 System Management 53
5.9.1 Password Setup 53
5.9.2 Upgrade 54
5.9.3 Reboot 54
5.9.4 Backup 54
5.9.5 Restore 55
5.9.6 WOL 55
5.9.7 System Time 56

Appendix A: FAQ 57

1. What and how to find my PC's IP and MAC address? 57
2. What is Wireless LAN? 57
3. What are ISM bands? 57
4. How does wireless networking work? 57
5. What is BSSID? 58
6. What is ESSID? 58
7. What are potential factors that may causes interference? 58
8. What are the Open System and Shared Key authentications? 59
9. What is WEP? 59
10. What is Fragment Threshold? 59
11. What is RTS (Request to Send) Threshold? 60
12. What is Beacon Interval? 60
13. What is Preamble Type? 60
14. What is SSID Broadcast? 60
15. What is Wi-Fi Protected Access (WPA)? 61
16. What is WPA2? 61
17. What is 802.1x Authentication? 61
18. What is Temporal Key Integrity Protocol (TKIP)? 61
19. What is Advanced Encryption Standard (AES)? 61
20. What is Inter-Access Point Protocol (IAPP)? 61
21. What is Wireless Distribution System (WDS)? 62
22. What is Universal Plug and Play (UPnP)? 62

23. What is Maximum Transmission Unit (MTU) Size? 62
24. What is Clone MAC Address? 62
25. What is DDNS? 62
26. What is NTP Client? 62
27. What is VPN? 62
28. What is IPSEC? 62
29. What is WLAN Block Relay between Clients? 63
30. What is WMM? 63
31. What is WLAN ACK TIMEOUT? 63
32. What is Modulation Coding Scheme (MCS)? 63
33. What is Frame Aggregation? 63
34. What is Guard Intervals (GI)? 63

Appendix B: Troubleshooting 64

Appendix C: Specifications 65

Appendix D: Glossary 67

Chapter 1. Product Introduction

1.1 Package contents

The following items should be contained in the package:

- WNAP-6306 Wireless Outdoor AP
- 18VDC PoE Injector (for EU/US region)
- 15VDC Power Adapter & PoE Injector (for UK/Other region)
- Quick Installation Guide
- CD-ROM (User's Manual included)

If there is any item missed or damaged, please contact the seller immediately.

1.2 Product Description

The WNAP-6306 is an affordable IEEE 802.11b/g /n specifications of Outdoor AP solution. It provides a setting of SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN. This document describes the steps required for the initial IP address assign and other configuration of the Outdoor AP.

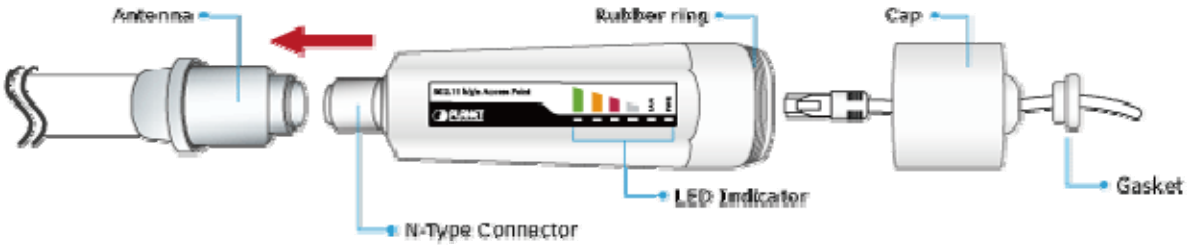
Flexible Outdoor Wireless Network

PLANET WNAP-6306 Wireless Outdoor Access Points brings users greatly more flexibility in extending outdoor wireless coverage as it is designed to be easily attached to the antenna directly. With built-in N-Type antenna connector, the WNAP-6306 can directly connect with various type and high gain antenna* to cover wide range and deliver much farther wireless connection over 10Km. Adopting IEEE 802.11n advanced 1T1R MIMO technology; the WNAP-6306 provides reliable wireless network coverage and incredible improvement in the wireless performance. It can deliver data rate up to 150Mbps, which is three times faster than normal 802.11g wireless devices.

* Available antenna models for the WNAP-6306: ANT-OM8, ANT-OM15, ANT-FP9, ANT-FP18, ANT-SE18, ANT-YG13, ANT-YG20, and ANT-GR21.

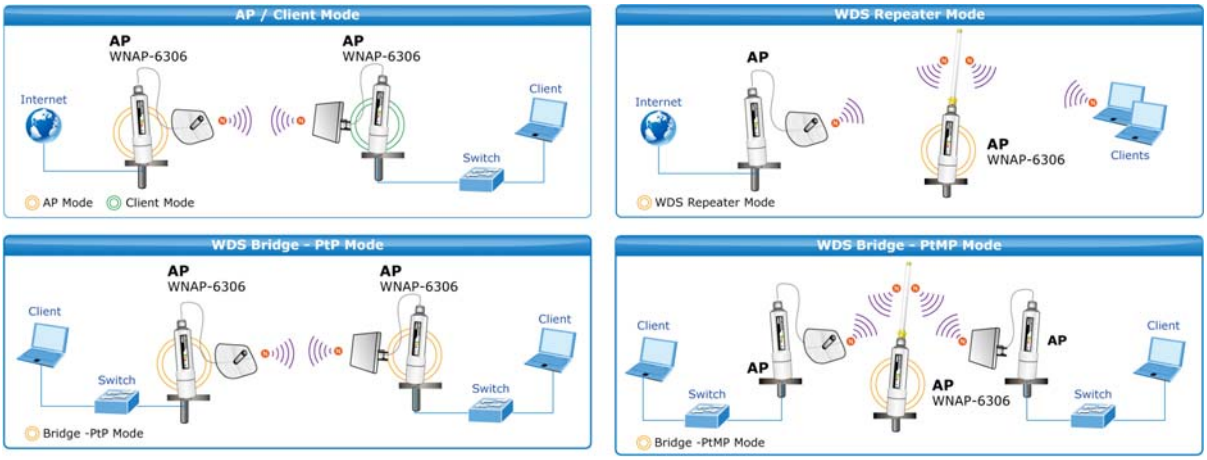
Easy Plug-n-Link

The WNAP-6306 especially benefits users to easily build outdoor wireless network with its Plug-n-Link capability via the built in N-Type antenna connector. The N-Type antenna connector is most commonly adapted with outdoor antenna and the mounting-free design of outdoor enclosure. Users can directly plug the WNAP-6306 into the mounted antenna, and then the wireless link is constructed immediately. Therefore, even users who never experience the wireless network installation can accomplish the wireless deployment quickly.



Multiple Operating & Wireless Modes

The WNAP-6306 supports multiple wireless communication connectivity (AP / Client CPE / WDS PtP / WDS PtMP / Repeater / Universal Repeater), allowing various applications and giving users more comprehensive experience. It also helps user to easily build wireless network and extend the wireless range of existing wireless network.



Advanced Security and Management

In aspect of security, besides 64/128-bit WEP encryption, the WNAP-6306 integrates WPA / WPA2, WPA-PSK and WPA2-PSK to protect your wireless LAN security. It provides wireless MAC filtering and SSID broadcast control to consolidate the wireless network security and prevent unauthorized wireless connection. Furthermore, the WNAP-6306 features the Dual-SSID function to enable you setup two different wireless networks with the WNAP-6306 serving as a virtual access point for segmented networks tailored to any office or industrial need.

Perfect Solution for Outdoor Environment

The WNAP-6306 is perfectly suitable to be installed in outdoor environments and exposed locations. With its IP65 casing protection, the WNAP-6306 can perform stably under rigorous weather conditions such as heavy rain and wind. The WNAP-6306 applies the proprietary Power over Ethernet (PoE) design, so it can be easily installed in any area where power outlets are unavailable. It is the best way using the WNAP-6306 to build outdoor wireless access applications between buildings on campuses, businesses, rural areas and etc.

1.3 Product Features

- **Industrial Compliant Wireless LAN & LAN**
  - Compliant with IEEE 802.11n wireless technology capable of up to 150Mbps data rate
  - Backward compatible with 802.11b/g standard
  - Equipped with 10/100Mbps RJ-45 LAN Port, Auto MDI/ MDI-X supported
  - Support DHCP Server, UPnP
- **RF Interface Characteristics**
  - Built-in N-Type Antenna Connector
  - High Output Power with multiple adjustable transmit power control
- **Outdoor Environmental Characteristics**
  - IP65 Enclosure
  - Passive Power Over Ethernet Design
  - Operating Temperature: -20 ~ 70°C
- **Multiple Operation & Wireless Mode**
  - Multiple Wireless Modes:
    - AP, Client
    - WDS PtP/PtMP
    - Repeater
    - Universal Repeater
  - Support Dual SSID
- **Secure Network Connection**
  - Support Software Wi-Fi Protected Setup (WPS)
  - Advanced security: 64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK(TKIP/AES)
  - Support MAC Filtering up to 20 clients
- **Easy Installation & Management**
  - User friendly Web-based UI with On-line Help
  - System status monitoring includes DHCP Client, Associated List, System Log
  - Wireless LED Thresholds for antenna alignment
  - Wake-On-LAN(WOL) to allow remotely wake up a WOL enabled host
  - Mounting-free design

1.4 Product Specification

Product	**WNAP-6306** 2.4GHz 802.11n Wireless Outdoor Access Point
Hardware Specification	
Standard support	IEEE 802.11b/g IEEE 802.11n IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3x Flow Control
Memory	16 Mbytes DDR SDRAM 4 Mbytes Flash
Interface	Wireless IEEE 802.11b/g/n LAN: 1 x 10/100Base-TX, Auto-MDI/MDIX
Antenna	Built-in N-Type (N-Male) Antenna Connector
Enclosure	IP65 waterproof case
PoE	Passive PoE 15~18V DC LAN RJ-45 Pin Assignment: PIN 4,5(+), PIN 7,8(-)
Dimension (D x H)	46 x 205 mm
Weight	192g
Wireless Interface Specification	
Frequency Band	2.4~2.4835GHz
Modulation	Transmission/Emission Type: DSSS / OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM, DBPSK, QPSK, CCK
Data Rate	802.11b: 11, 5.5, 2 and 1 Mbps with auto-rate fall back 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6Mbps 802.11n (20MHz): up to 72Mbps 802.11n (40MHz): up to 150Mbps
Opt. Channel	America/ FCC: 2.414~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels) Japan/ TELEC: 2.412~2.484GHz (14 Channels)
RF Output Power	802.11b: 20 ± 1dBm 802.11g: 19 ± 1dBm 802.11n: 16 ± 1dBm
Receiver Sensitivity	802.11b: -84dBm 802.11g: -68dBm 802.11n (20MHz): -65dBm 802.11n (40MHz): -62dBm
Media Access Control	CSMA/CA

Output Power Control	Range 1~100, default:100
Power Requirements	15~18V DC, 1A (switching)
Wireless Management Features	
Wireless Mode	■ AP ■ Client ■ WDS PtP ■ WDS PtMP ■ WDS Repeater (AP+WDS) ■ Universal Repeater (AP+Client)
Channel Width	20MHz / 40MHz
Encryption Security	64/128-bits WEP WPA, WPA-PSK WPA2, WPA2-PSK
AP Isolation/WLAN Partition	Able to isolate each connected wireless client from each other to access mutually.
Wireless Security	Wireless MAC address filtering
	WPS (WiFi Protected Setup)
	Enable/Disable SSID Broadcast
B/G Protection Mode	A protection mechanism prevents collisions among 802.11b/g modes
Association List	Display current status of the wireless client associated with AP
Max. Wireless Client	25
Max. WDS AP	4
Software	
LAN	Built-in DHCP server supporting static IP address distributing
	DHCP Reserve
Access Control	MAC filtering up to 20 MAC address
Max. Wired Client	60
Applications & Game	UPnP support
Management	Web UI, DHCP Client, WOL
Diagnostic tool	System Log
Environment & Certification	
Operation	Temperature: -20~70 Degree C Humidity: 10~95% non-condensing
Storage	Temperature: -30~80 Degree C Humidity: 5~95% non-condensing
Regulatory	CE / RoHS

1.5 Wireless Performance

The following information will help you utilizing the wireless performance, and operating coverage of WNAP-6306.

1. Site selection

To avoid interferences, please locate WNAP-6306 and wireless clients away from transformers, microwave ovens, heavy-duty motors, refrigerators, fluorescent lights, and other industrial equipments. Keep the number of walls, or ceilings between AP and clients as few as possible; otherwise the signal strength may be seriously reduced. Place WNAP-6306 in open space or add additional WNAP-6306 as needed to improve the coverage.

2. Environmental factors

The wireless network is easily affected by many environmental factors. Every environment is unique with different obstacles, construction materials, weather, etc. It is hard to determine the exact operating range of WNAP-6306 in a specific location without testing.

Chapter 2. Hardware Description

2.1 LED Panel

Figure 2-1 Rear Panel LED Identification

2.2 LED Indications

LED		State	Meaning
Power		On	System On
		Off	System Off
LAN		On	LAN Port linked.
		Off	No link.
		Blinking	Data is transmitting or receiving on the LAN interface.
Signal Indicator	LED1	On	The wireless Signal Strength reaches the value
	LED2	On	The wireless Signal Strength reaches the value
	LED3	On	The wireless Signal Strength reaches the value
	LED4	On	The wireless Signal Strength reaches the value

2.3 Port & Connector

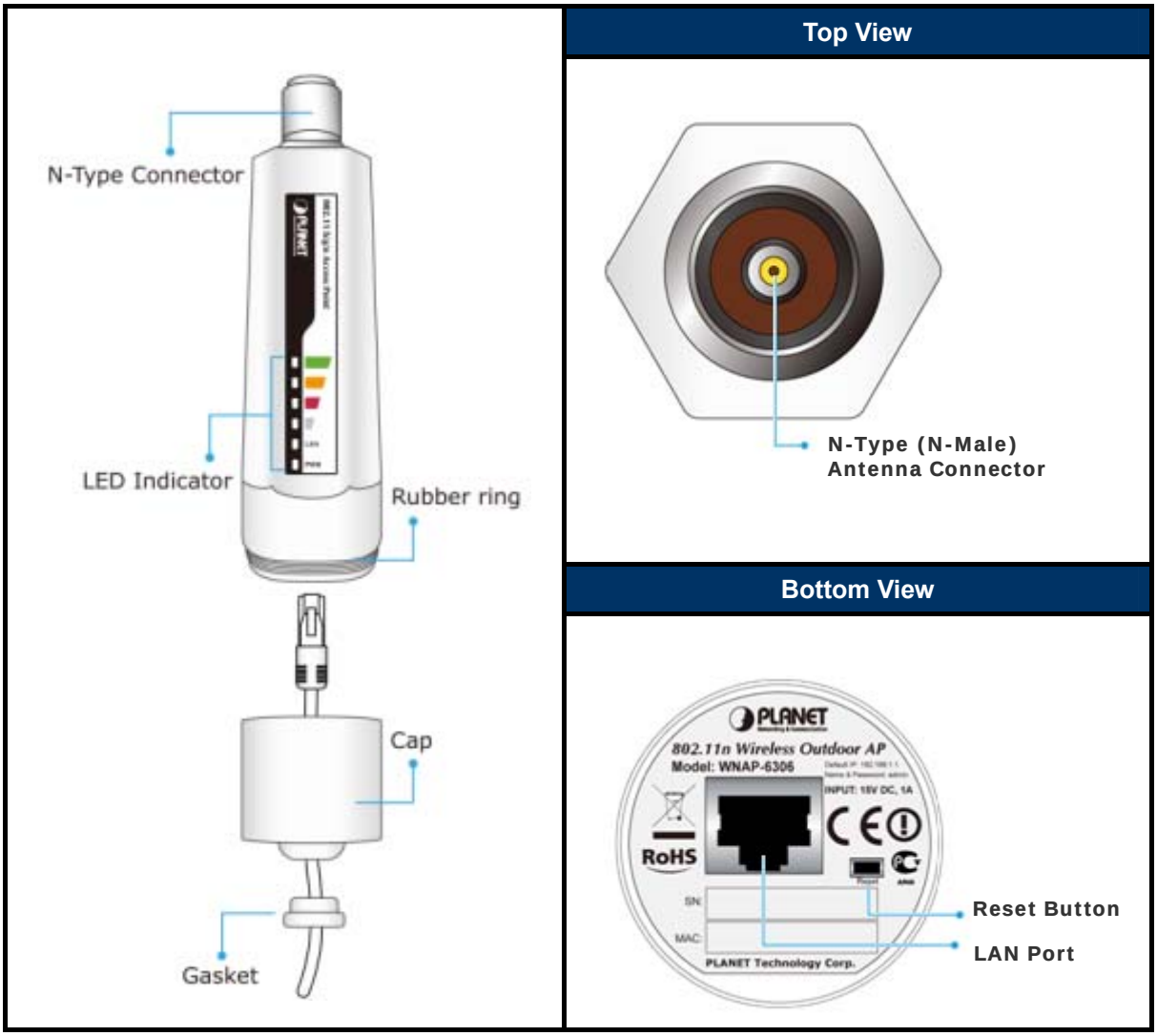


Figure 2-2 Port and Connector of WNAP-6306

Interface	Function
N-Type Connector	For external antenna. You can use the N-Type connector to connect with 2.4GHz external antenna.
LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
Reset	Push continually the reset button of POE injector about 2 ~ 6 seconds to reset the configuration parameters to factory defaults.

Please physically attach antenna before power on.

2.4 PoE Injector

18VDC PoE Injector	PoE Warning Label
※The 18VDC PoE Injector is for EU & US regions.	

Figure 2-3 18VDC PoE Injector

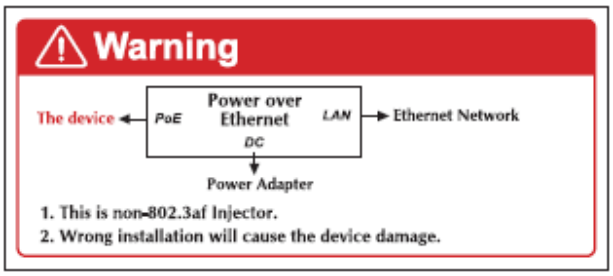
15VDC Power Adapter & PoE Injector	PoE Warning Label
	
※The 15VDC Power Adapter & PoE Injector are for UK & Other regions.	

Figure 2-4 15VDC Power Adapter & PoE Injector

Chapter 3. Hardware installation

This chapter describes safety precautions and product information you have to know and check before installing WNAP-6306.

3.1 Preparation before Installation

3.1.1 Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

3.1.2 Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing WNAP-6306 for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing WNAP-6306, please note the following things:
   - Do not use a metal ladder;
   - Do not work on a wet or windy day;
   - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

3.1.3 Installation Precautions

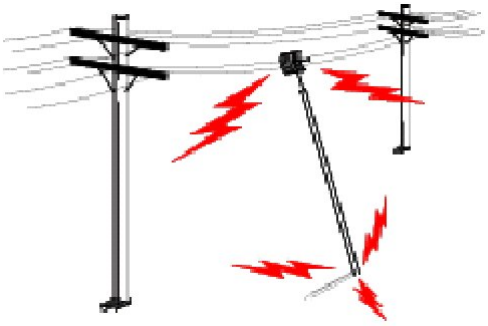
1. Users **MUST** use a proper and well-installed surge arrestor and grounding kit with WNAP-6306; otherwise, a random lightening could easily cause fatal damage to WNAP-6306. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**
2. Users **MUST** use the "AC Adapter & PoE Injector" shipped in the box with the WNAP-6306. Use of other options will cause damage to the WNAP-6306.
3. Users **MUST** power off the WNAP-6306 first before connecting the antenna to it, otherwise, damage might be caused to the WNAP-6306 itself.
4. The Antenna is required, and must be purchased separately.
5. No enclosure mounting is required, just the Antenna need to be mounted properly.

OUTDOOR INSTALLATION WARNING

IMPORTANT SAFETY PRECAUTIONS:

LIVES MAY BE AT RISK! Carefully observe these instructions and any special instructions that are included with the equipment you are installing.

CONTACTING POWER LINES CAN BE LETHAL. Make sure no power lines are anywhere where possible contact can be made. Antennas, masts, towers, guy wires or cables may lean or fall and contact these limes. People may be injured or killed if they are touching or holding any part of equipment when it contacts electric lines. Make sure there is NO possibility that equipment or personnel can come in contact directly or indirectly with power lines.



Assume all overhead lines are power lines.

The horizontal distance from a tower, mast or antenna to the nearest power line should be at least twice the total length of the mast/antenna combination. This will ensure that the mast will not contact power if it falls either during installation or later.

TO AVOID FALLING, USE SAFE PROCEDURES WHEN WORKING AT HEIGHTS ABOVE GROUND.

- Select equipment locations that will allow safe, simple equipment installation.
- Don't work alone. A friend or co-worker can save your life if an accident happens.
- Use approved non-conducting lasers and other safety equipment. Make sure all equipment is in good repair.
- If a tower or mast begins falling, don't attempt to catch it. Stand back and let it fall.
- If anything such as a wire or mast does come in contact with a power line, **DON'T TOUCH IT OR ATTEMPT TO MOVE IT**. Instead, save your life by calling the power company.
- Don't attempt to erect antennas or towers on windy days.

MAKE SURE ALL TOWERS AND MASTS ARE SECURELY GROUNDED, AND ELECTRICAL CABLES CONNECTED TO ANTENNAS HAVE LIGHTNING ARRESTORS. This will help prevent fire damage or human injury in case of lightning, static build-up, or short circuit within equipment connected to the antenna.

- The base of the antenna mast or tower must be connected directly to the building protective ground or to one or more approved grounding rods, using 1 OAWG ground wire and corrosion-resistant connectors.
- Refer to the National Electrical Code for grounding details.

IF A PERSON COMES IN CONTACT WITH ELECTRICAL POWER, AND CANNOT MOVE:

- **DON'T TOUCH THAT PERSON, OR YOU MAY BE ELECTROCUTED.**
- Use a non-conductive dry board, stick or rope to push or drag them so they no longer are in contact with electrical power.

Once they are no longer contacting electrical power, administer CPR if you are certified, and make sure that emergency medical aid has been requested.

3.2 Hardware Installation

3.2.1 Connect Up

Step 1. Connect the Antenna to the top of WNAP-6306.

Figure 3-1 Connect Antenna

Step 2. (1) Open the bottom of WNAP-6306.

(2) Plug the RJ-45 Ethernet cable into the LAN Port through the Cap and Gasket. Then seal the bottom of the WNAP-6306 with the Cap and Gasket.

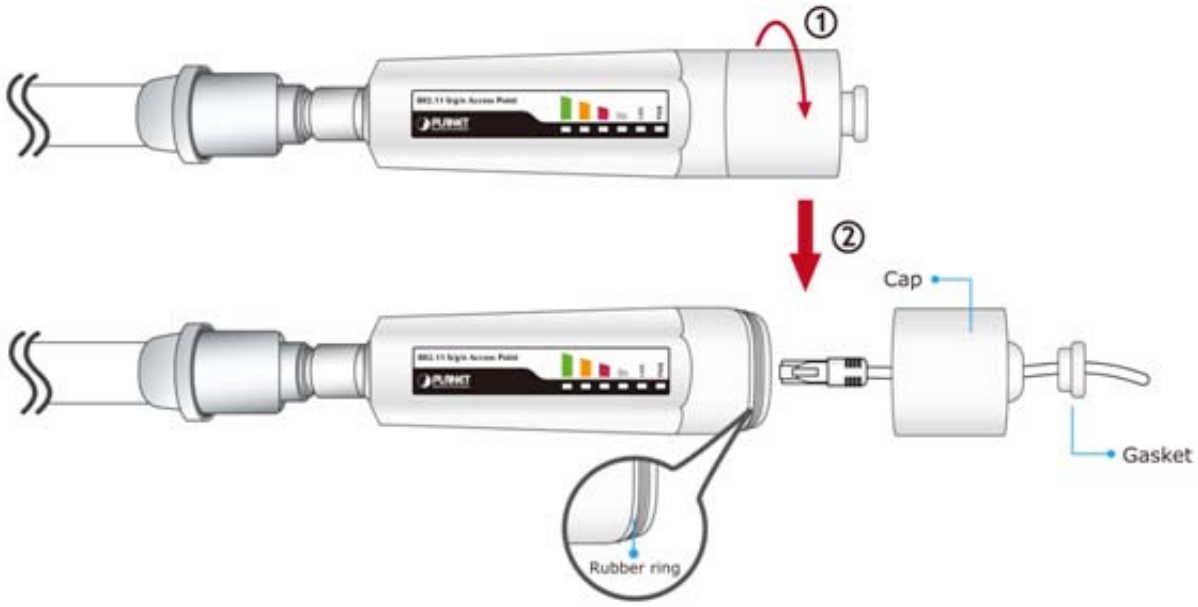


Figure 3-2 Cable Connection

Note

1. Ensure to pack the Gasket into the Cap tightly to avoid the penetration of water.
2. Do not remove or lose the Rubber ring that fits over the spiral groove on the bottom of the WNAP-6306, otherwise, the product may be damaged by the penetration of water.
3. RJ-45 8P8C Ethernet cable is required.

Step 3. (1) Plug the other side of the RJ-45 cable in the STEP 2 into the PoE port of the PoE Injector.

(2) Plug another RJ-45 cable into the LAN port of PoE Injector, and the other side plug into the LAN port of PC or Switch.

(3) Plug the 18V PoE Injector into the Power Outlet. For UK and other regions, you need to supply the power by the 15V AC Adapter.

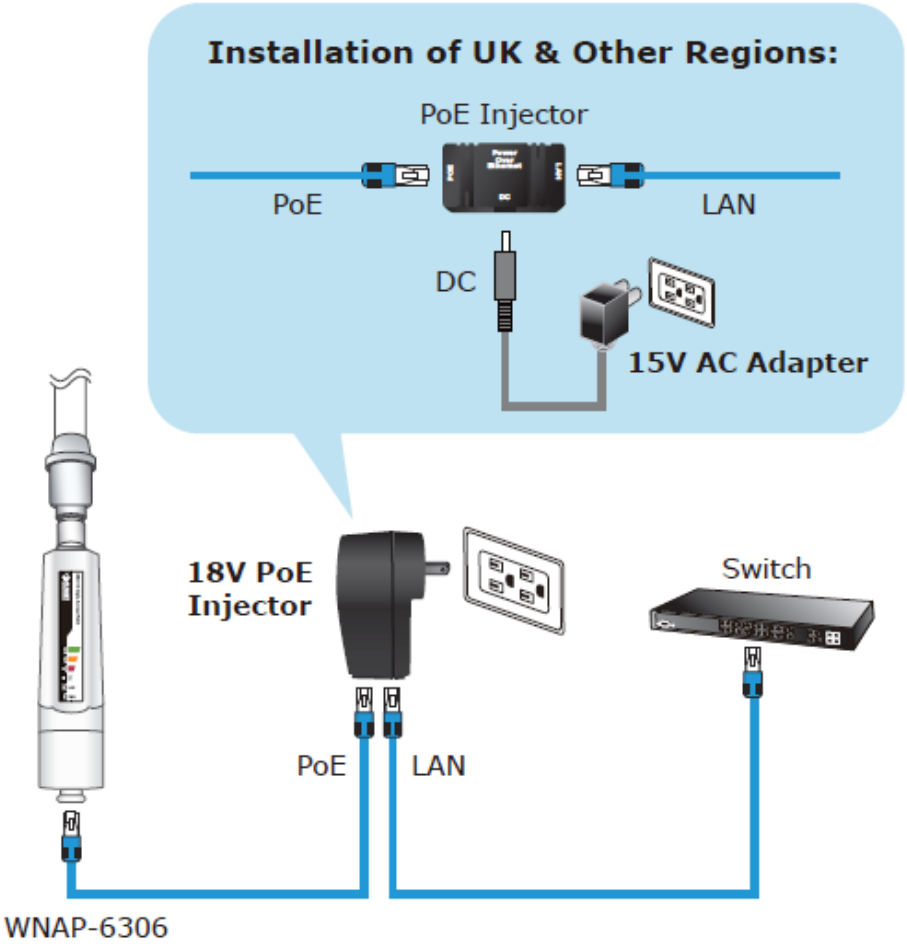


Figure 3-3 PoE Installation

Note

1. It will take about 30 seconds to complete the boot up sequence after powered on the Outdoor AP; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.
2. Be reminded, the UTP wire distance toward your WNAP-6306 to the Ethernet devices, such as Ethernet Switch, is 100 meters, the passive POE injector can be in any point of this 100 meters UTP distance where there is a shell or protected location.
3. To avoid thunder strike, consider to install ELA-100, thunder arrester toward the CPE AP and the PoE injector.

Chapter 4. Software Installation

4.1 Software Configuration

There are web based management and configuration functions allowing you to have the jobs done easily. The WNAP-6306 is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: 192.168.1.1
Default IP subnet mask: 255.255.255.0
WEB login User Name: admin
WEB login Password: admin

4.2 Connecting the AP

For OS of Microsoft Windows 2000/ XP:

1. Click the ***Start*** button and select Settings, then click ***Control Panel***. The *Control Panel* window will appear.

2. Move mouse and double-click the right button on ***Network and Dial-up Connections*** icon. Move mouse and double-click the ***Local Area Connection*** **icon**. The *Local Area Connection* window will appear. Click ***Properties*** button in the *Local Area Connection* window.

Figure 4-1

3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.

4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click *Add* button.

5. Select ***TCP/IP*** in Microsoft of Select ***Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.

6. Select ***TCP/IP*** and click the properties button on the ***Network*** dialog box.

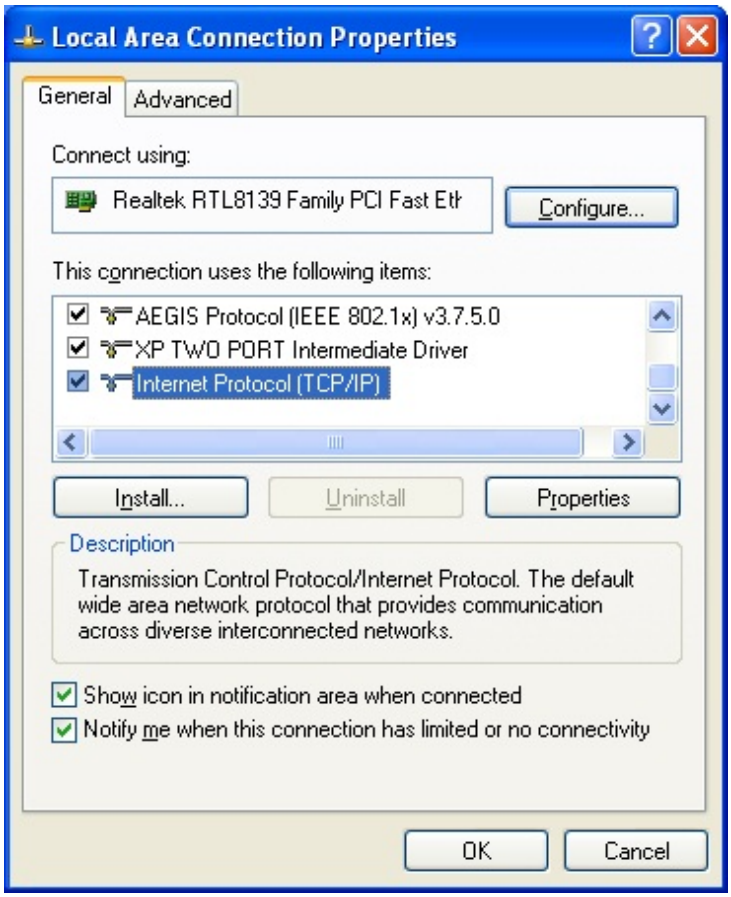


Figure 4-2

7. Select Specify an IP address and type in values as following example.

   IP Address: *192.168.1.2*, any IP address within 192.168.1.2 to 192.168.1.254 is good to connect the Wireless LAN Access Point.

   IP Subnet Mask: *255.255.255.0*

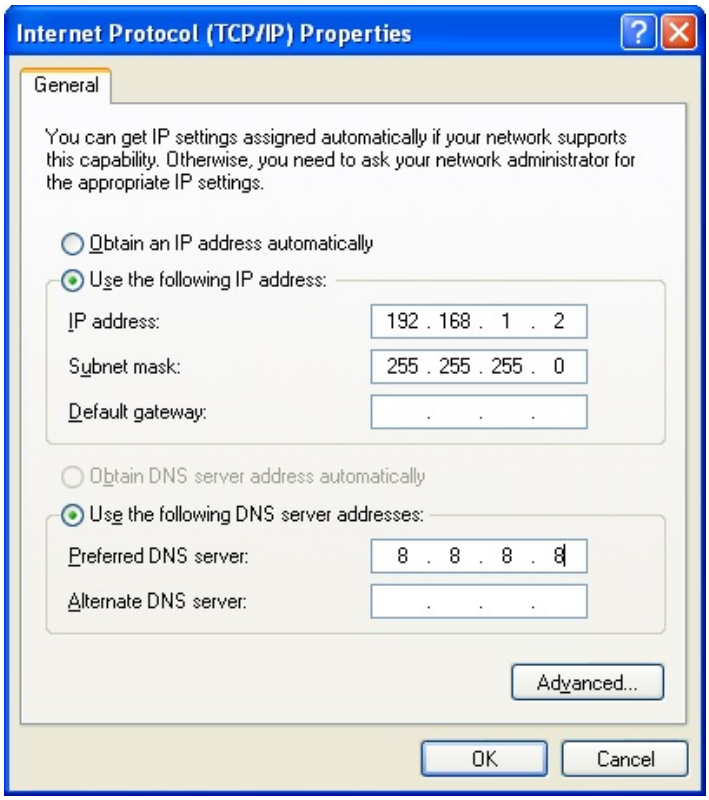


Figure 4-3

8. Click ***OK*** to complete the IP parameters setting.

For OS of Microsoft Windows Vista / 7:

1. Click the *Start* button and select *Settings*, then click ***Control Panel***. The *Control Panel* window will appear.

2. Move mouse and double-click the right button on ***Network Connections*** item. The *Network Connections* window will appear. Double click ***Local Area Connection*** **icon**, then User Account Control window shown. Right click Continue button to set properties.

3. In ***Local Area Connection Properties*** window, Choose ***Networking*** tab, move mouse and click ***Internet Protocol Version 4 (TCP/IPv4)***, then click *Properties* button.

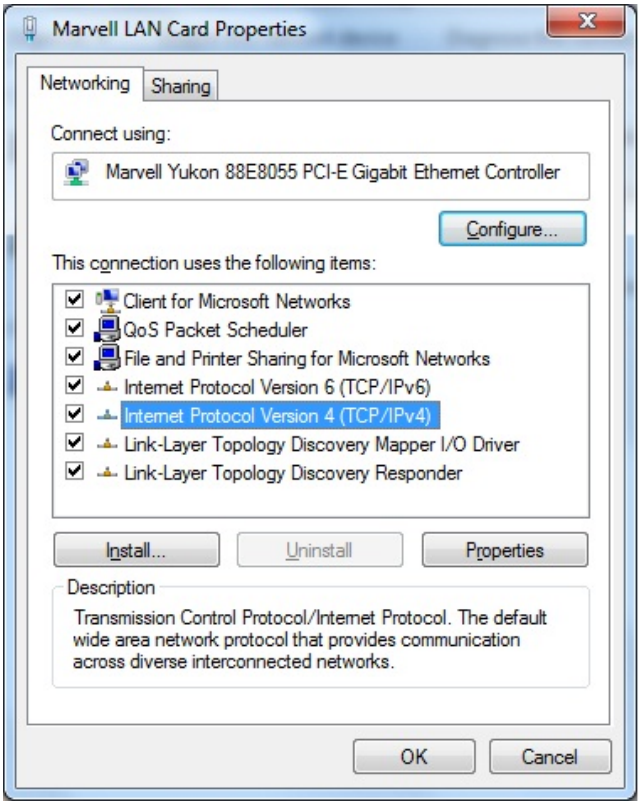


Figure 4-4

4. Move mouse and click ***General*** tab, Select ***Specify an IP address*** and type in values as following example.

   IP Address: *192.168.1.2*, any IP address within 192.168.1.2 to 192.168.1.254 is good to connect the Wireless LAN Access Point. IP Subnet Mask: *255.255.255.0*

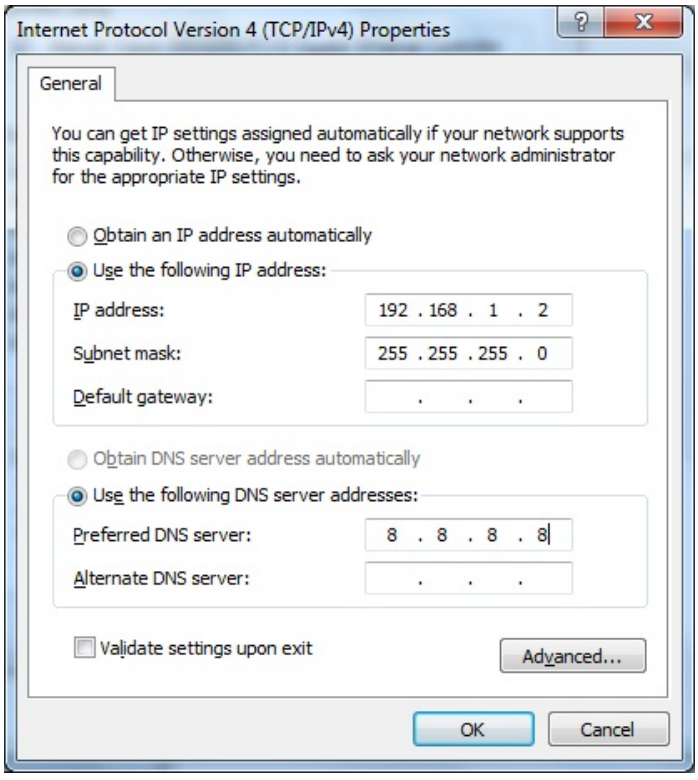


Figure 4-5

5. Click **OK** to complete the IP parameters setting.

For OS of Microsoft Windows NT:

1. Click the *Start* button and select Settings, then click *Control Panel*. The *Control Panel* window will appear.
2. Move mouse and double-click the right button on Network icon. The Network window will appear. Click Protocol tab from the Network window.
3. Check the installed list of Network Protocol window. If TCP/IP is not installed, click the Add button to install it; otherwise go to step 6.
4. Select Protocol in the Network Component Type dialog box and click Add button.
5. Select *TCP/IP* in *Microsoft of Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
6. Select *TCP/IP* and click the properties button on the *Network* dialog box.
7. Select Specify an IP address and type in values as following example.

   IP Address: *192.168.1.2*, any IP address within 192.168.1.2 to 192.168.1.254 is good to connect the Wireless LAN Access Point.

   IP Subnet Mask: *255.255.255.0*
8. Click *OK* to complete the IP parameters setting.

4.3 Web Login

Open a WEB browser, i.e. Microsoft Internet Explore 6.1 SP1 or above, then enter **192.168.1.1** on the URL to connect the WNAP-6306.

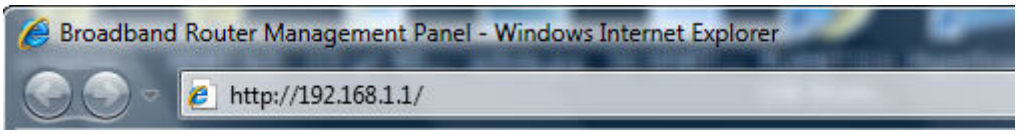


Figure 4-6

After a moment, a login window will appear. Enter the User Name and Password. Then click the **OK** button.

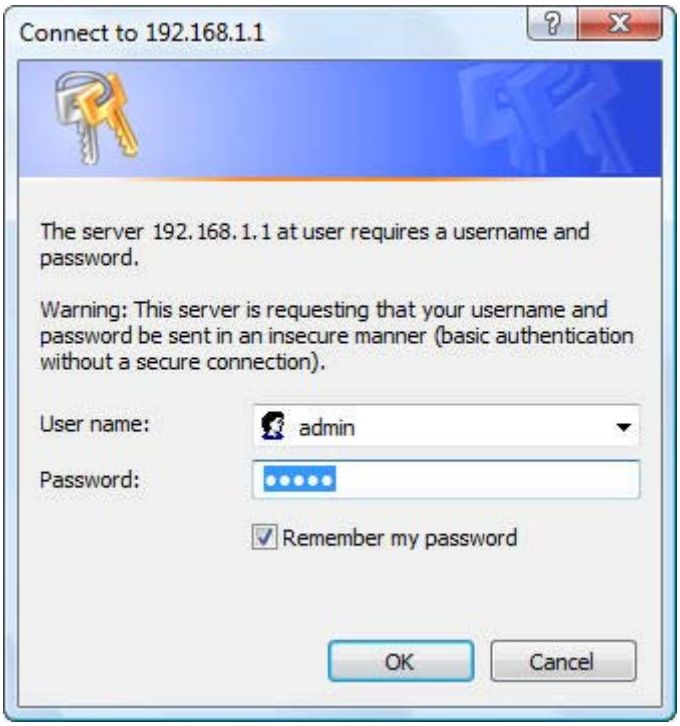


Figure 4-7 Login Window

Default User name: **admin**
Default Password: **admin**

Note

If the above screen does not pop up, it may mean that your web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

After you enter the username and password, the main screen appears as Figure 4-8.

Figure 4-8 Web UI Screenshot

The next chapter will introduce the functions of the web UI.

Chapter 5. Basic System Settings

5.1 System Information

This System Information page provides running status information and detailed information.

5.1.1 System

This item provides current running information of System.

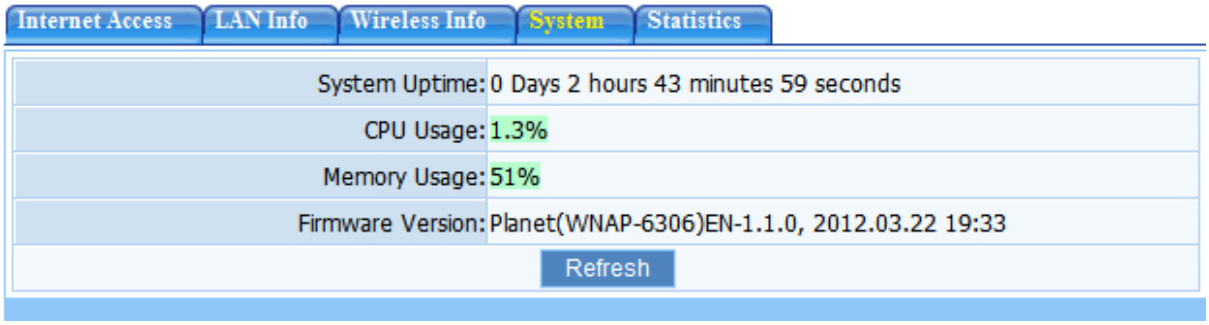


Figure 5-1 System

5.1.2 LAN Info

This item provides information about AP's LAN port, display LAN port's physical address, IP address and current situation of DHCP server.

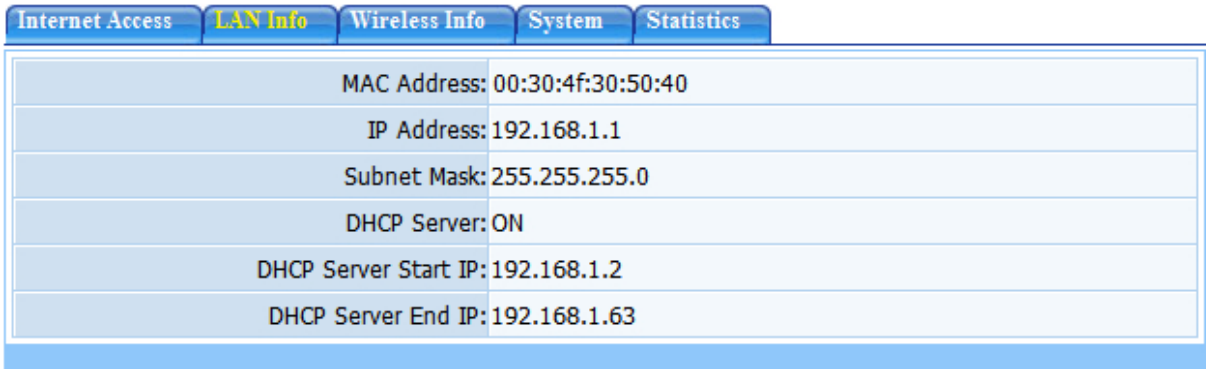


Figure 5-2 LAN Info

5.1.3 Wireless Info

This item provides current running information of wireless.

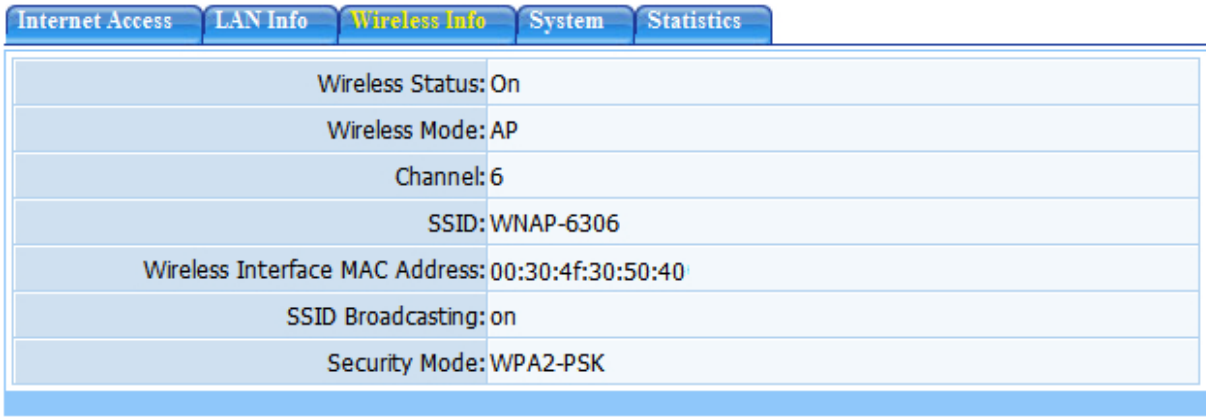


Figure 5-3 Wireless Info

The page includes the following fields:

Object	Description
Wireless Status	Display wireless interface status is enabled or not
Wireless Mode	Current wireless mode of wireless AP
Channel	Display current channel of your wireless AP.
SSID	SSID (Service Set Identifier) is your wireless network's name shared among all points in a wireless network.
MAC Address	The MAC address is used for wireless communication

5.1.4 Secondary AP

This item provides current running information of Secondary AP.

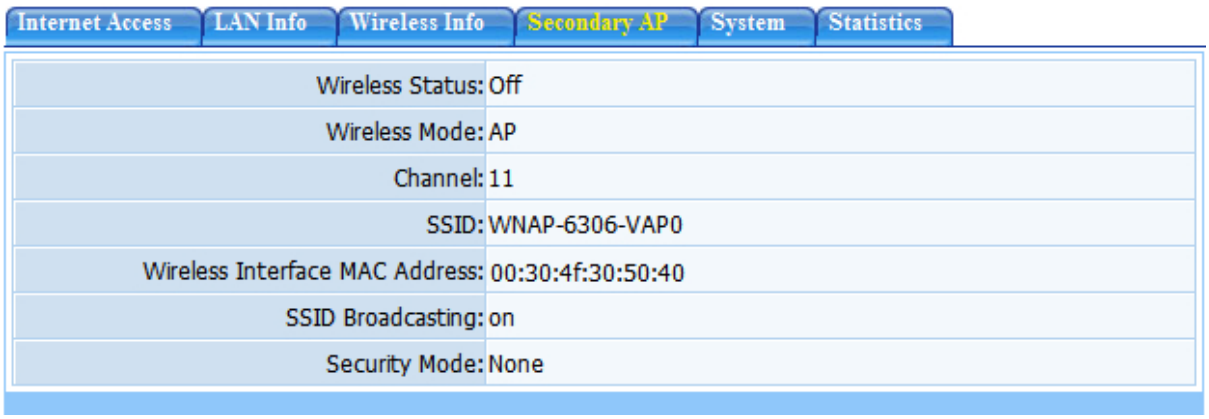


Figure 5-4 Secondary AP

5.1.5 Statistics

This item provides statistics information about the bits AP sends and received.

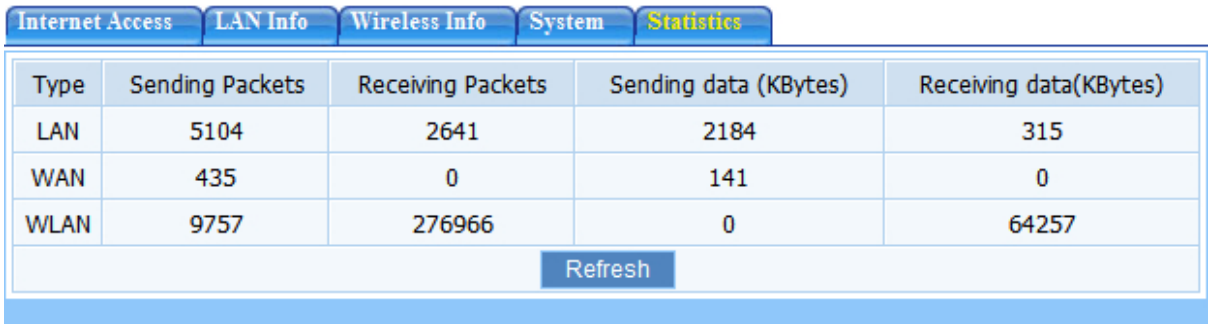


Figure 5-5 Statistics

5.2 System Log

View the system log. You can set the number of records per page, default is 10.

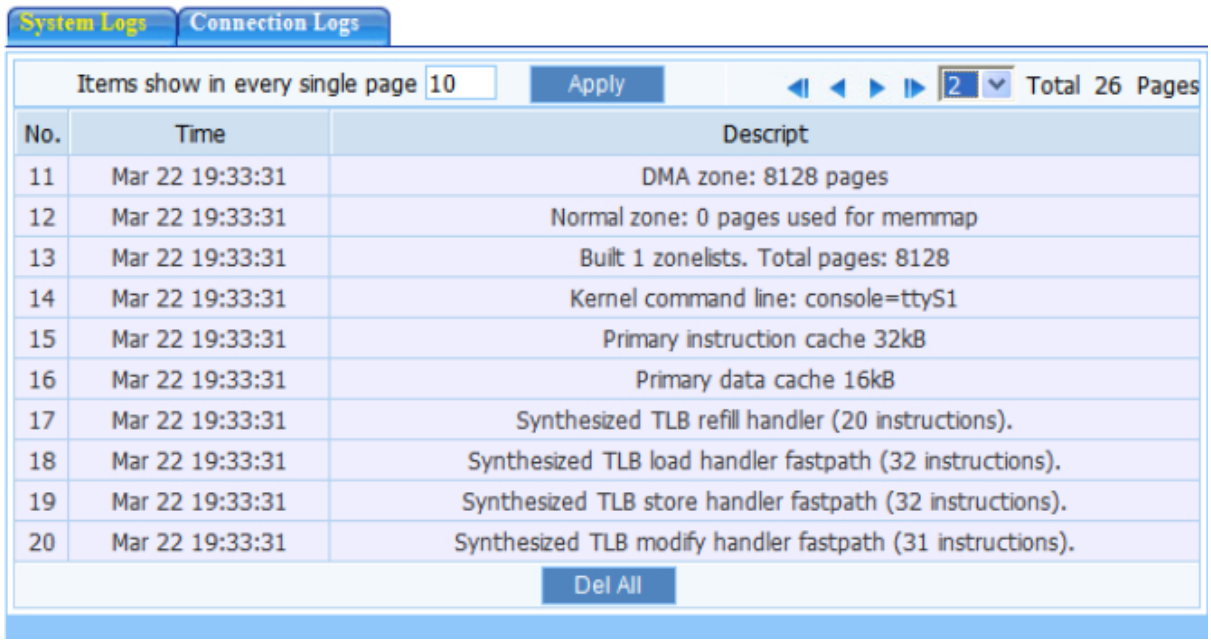


Figure 5-6 System Log

5.3 Internet Setup

5.3.1 WISP

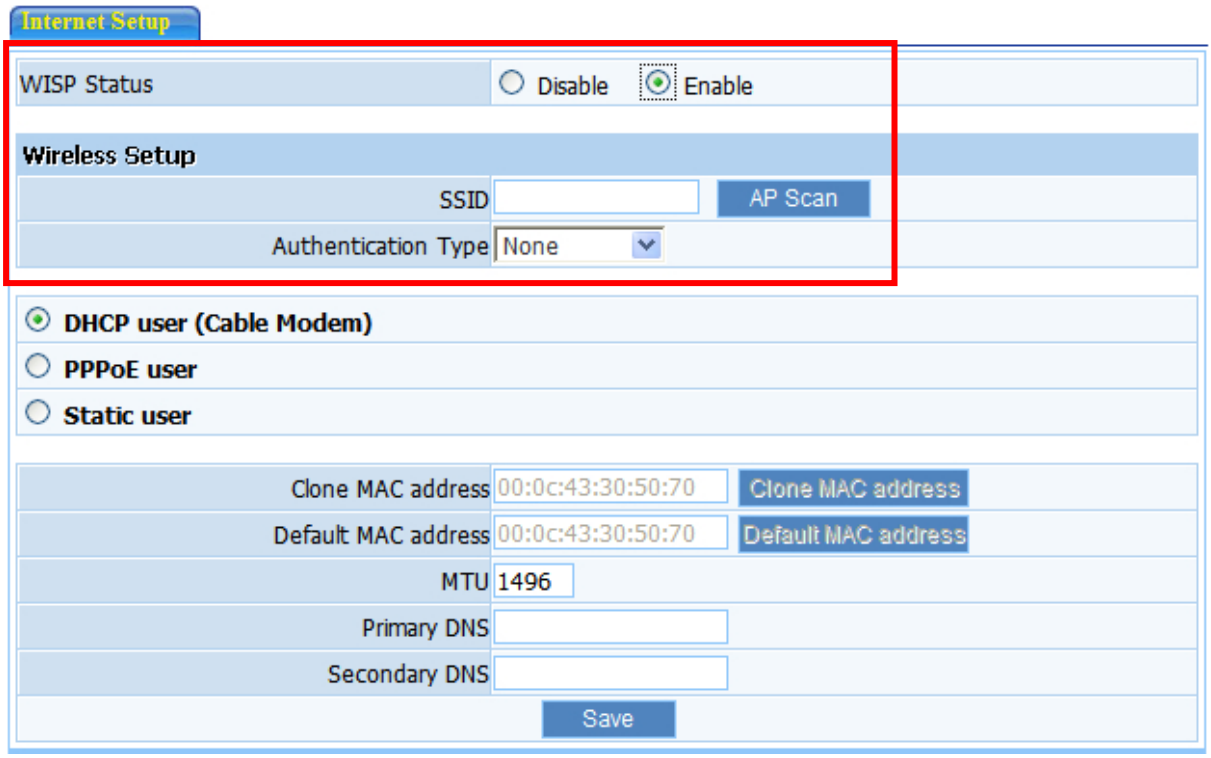


Figure 5-7 WISP

The page includes the following fields:

Object	Description
WISP Status	You can choose "enable" or "disable" to enable or disable the "WISP". The **Wireless ISP (WISP)** mode allows that the wireless interface is treated as WAN port, and the Ethernet port is LAN port. User must configure wireless encryption connection and set the Radio Mode to "**Client**".
SSID	You can manually enter the SSID of the Wireless AP that you want to connect, or click "**AP Scan**" to site survey a AP.
Authentication Type	Select the correct Authentication Type that should be the same as the Wireless AP that you want to connect to.

5.3.2 WAN Type

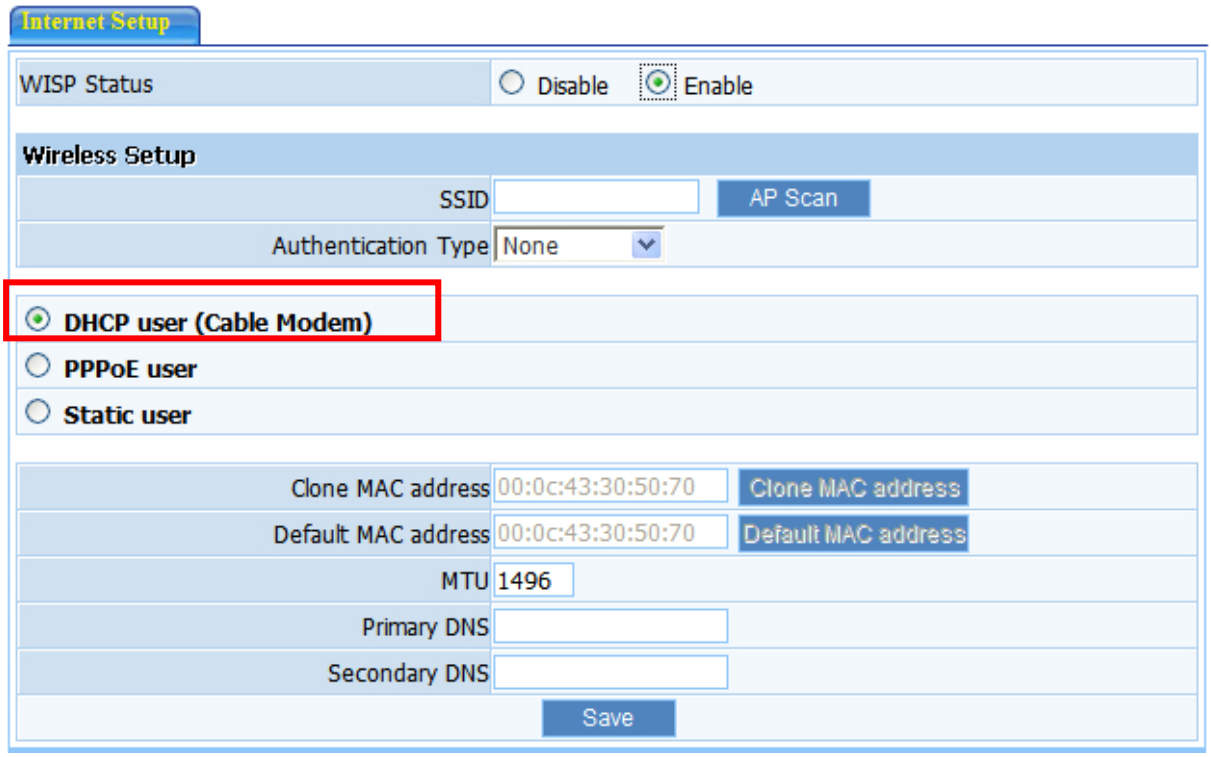


Figure 5-8 DHCP user (Cable Modem)

A. DHCP user (Cable Modem)

The DHCP user includes the following fields:

Object	Description
DHCP user (Cable Modem)	If your ISP provides the DHCP service, please choose **DHCP user (Cable Modem)** option, and the AP ill automatically obtain IP parameters from your ISP.
Clone MAC address	Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.
Default MAC address	Use Default MAC address to register to a server machine.
MTU	Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. It is not recommended that you change the default MTU Size unless required by your ISP.
Primary/Secondary DNS	(Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

B. PPPoE user

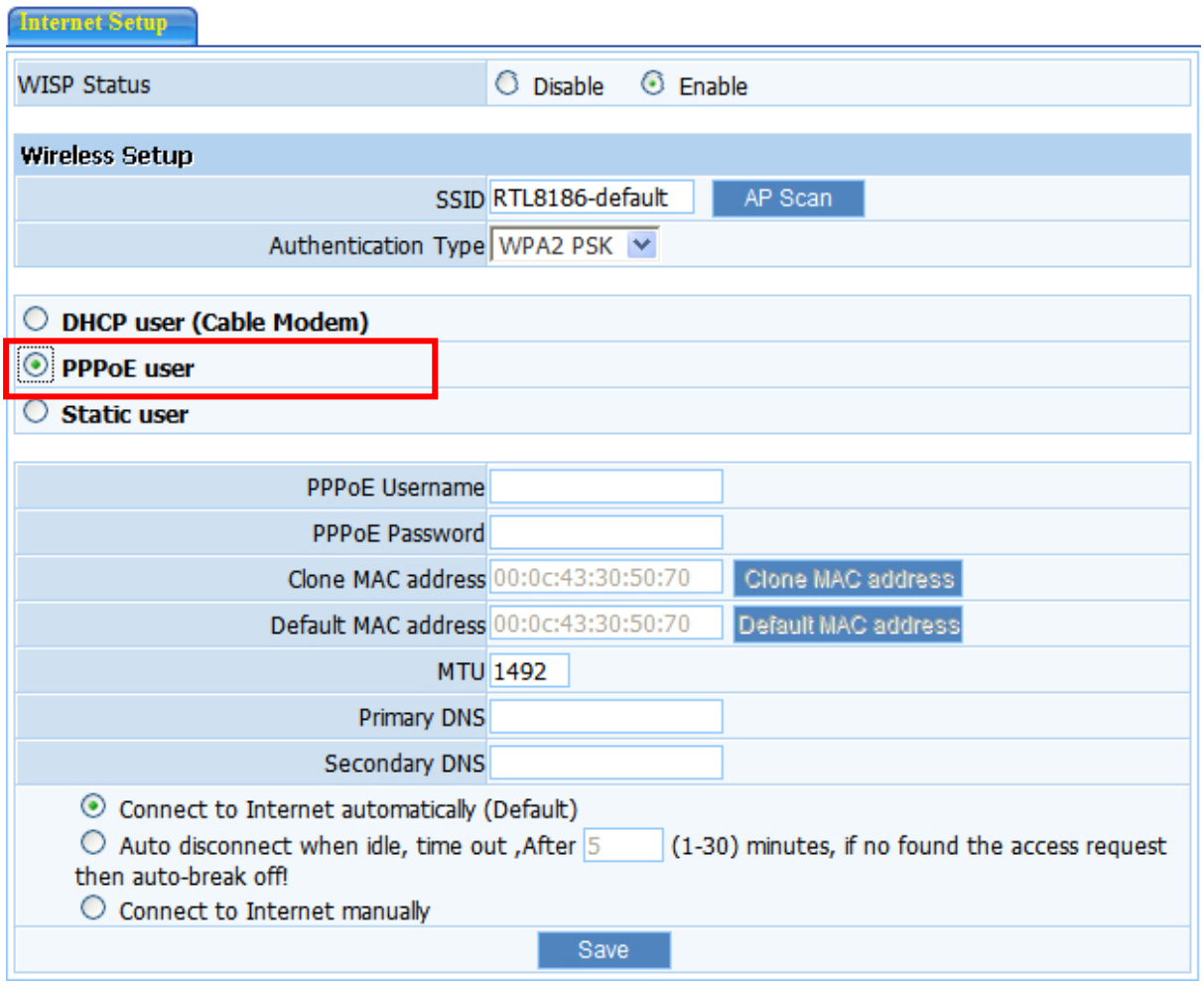


Figure 5-9 PPPoE user

The PPPoE user includes the following fields:

Object	Description
PPPoE user	If your ISP provides a PPPoE connection, select **PPPoE user** option.
PPPoE Username/Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
Clone MAC address	Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.
Default MAC address	Use Default MAC address to register to a server machine.
MTU	Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. It is not recommended that you change the default MTU Size unless required by your ISP.

Primary/Secondary DNS	(Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

C. Static user

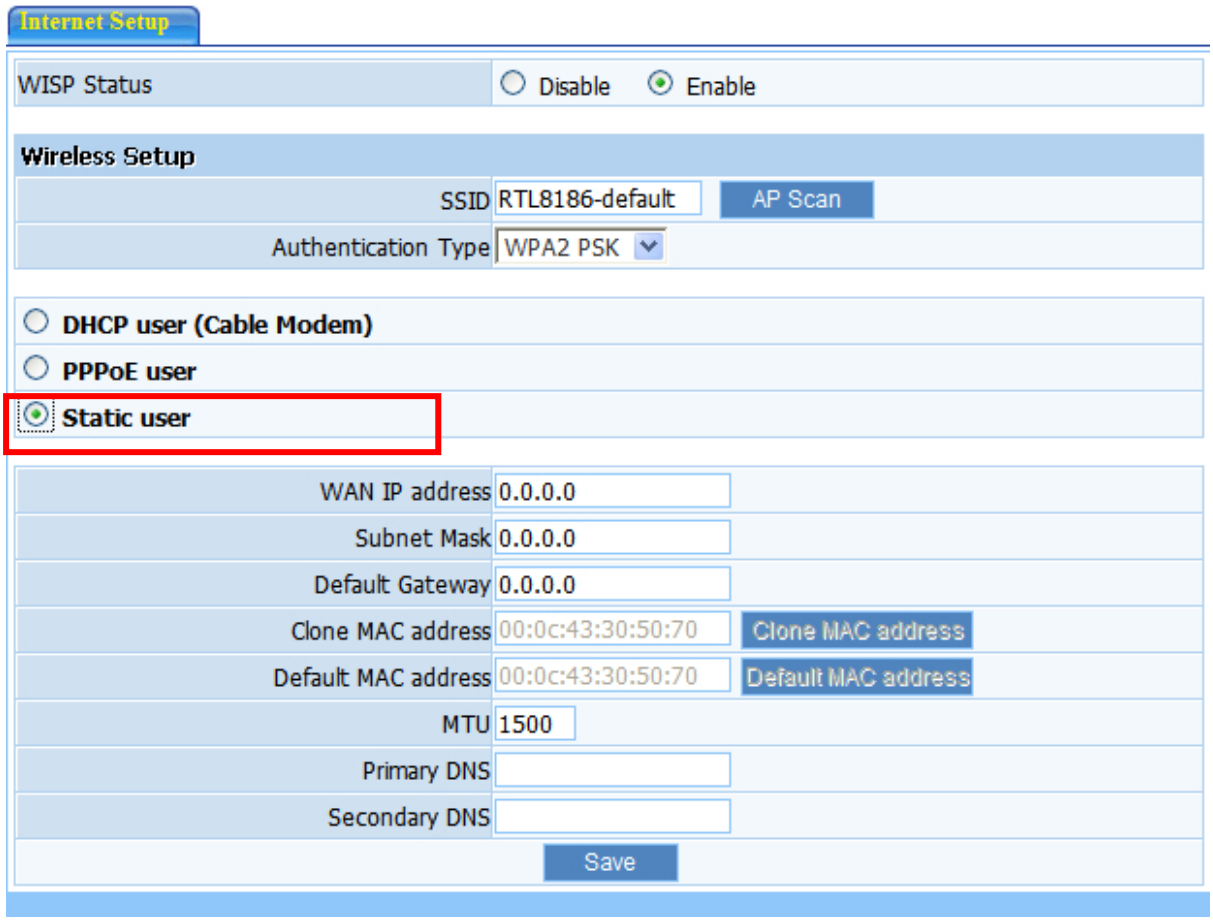


Figure 5-10 Static user

The Static user includes the following fields:

Object	Description
Static user	If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static user** option.
WAN IP address	Enter the IP address in dotted-decimal notation provided by your ISP.
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Default Gateway	(Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
Clone MAC address	Clone MAC address is designed for your special application that request the clients to register to a server machine with one

	identified MAC address.
Default MAC address	Use Default MAC address to register to a server machine.
MTU	Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. It is not recommended that you change the default MTU Size unless required by your ISP.
Primary/Secondary DNS	(Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

5.4 Wireless Management

Providing basic configuration items for wireless AP users, including "**wireless network status**", "**SSID**", "**Radio Band**", "**Radio Mode**", "**MAC**", "**SSID broadcasting**", "**Channel width**", "**Channel sideband**", "**Region"** and **"Channel**" several basic configuration items.

5.4.1 Wireless Setup

5.4.1.1 Basic

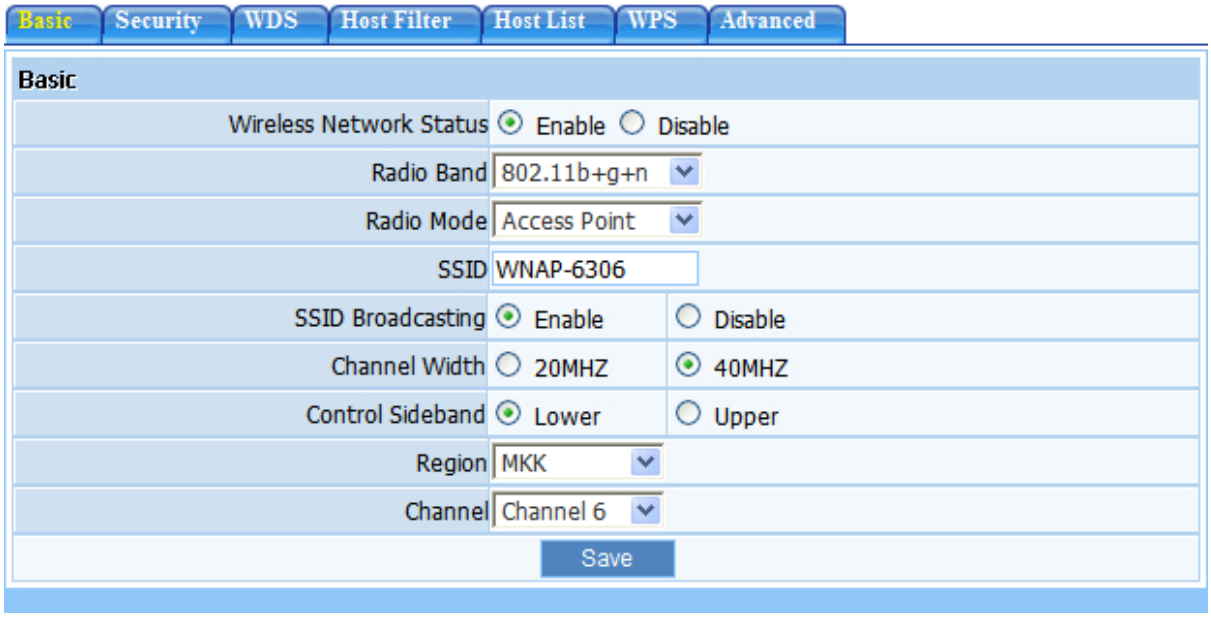


Figure 5-11 Wireless Basic Setting

The page includes the following fields:

Object	Description
Wireless network status	You can choose "enable" or "disable" to enable or disable the "Wireless Network Status", if what you choose is "Disable", the AP function of

	wireless AP will be turned off.
Radio band	You can select the wireless standards running on your network, if you have Wireless-N, and Wireless-B/G devices in your network, keep the default setting to "**802.11b+g+n**".
Radio mode	You can select radio mode of wireless AP, it contains Access Point, Client, AP+WDS, Repeater and Lazy. The default setting is AP mode.
SSID	The default SSID is **"Default".**
SSID Broadcasting	You can select "enable" or "disable" to enable or disable the broadcast SSID function, If the setting of this field is disable, wireless client can't obtain this SSID to login in, then user have to input the SSID value manually.
Channel width	This switch allows you to set AP's wireless bandwidth. 20MHz: In this mode you can get low bandwidth, little interference and slow rate. 40MHz: In this mode you can get high bandwidth, high interference and rapid rate.
Channel sideband	It controls your wireless AP use higher or lower channel when working on 40MHz.
Region	please select the region where you live in.
Channel	In 20MHz, you can select one channel from 1 to 13 manually, and in 40MHz, you can select one channel from 1 to 9 or 5 to 13, which provides a choice of avoiding interference.

5.4.1.2 Security

The item allows you to encrypt your wireless communication, and you can also protect your wireless network from unauthorized user access. It supplies "None", "WEP", "WPA-PSK", "WPA2-PSK" and "WPA/WPA2-PSK" five different encryption modes.

A. None

"None" means do not encrypt wireless data.

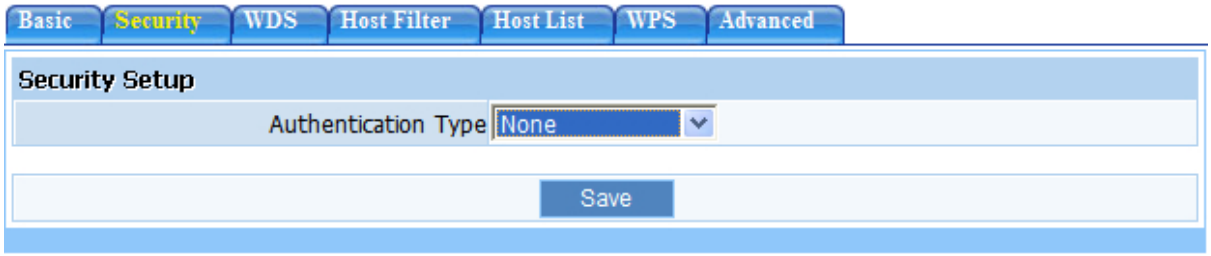


Figure 5-12 Security-None

B. WEP

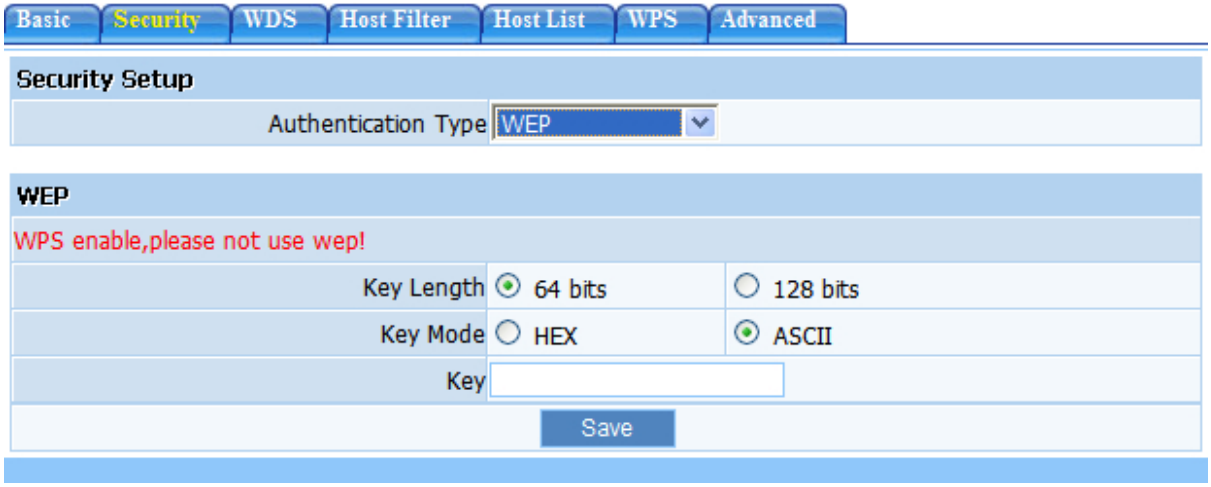


Figure 5-13 Security-WEP

The page includes the following fields:

Object	Description
Key Length	There are two basic levels of WEP encryption, 64 bits and 128 bits, the more bits password have, the better security wireless network is, at the same time the speed of wireless is more slower.
Key Mode	If you select WEP to encrypt your data, choose the bits of password, it should be 64 bits or 128 bits. Then choose the format of password; it should be HEX or ASCII. The valid character for HEX format should be numbers from 0 to 9 and letters from A to F. HEX support mixed letter and number mode. And ASCII supports all characters that in keyboard.
Key Length description	When you select 64bits, you need to input 10 chars for HEX and 5 chars for ASCII, and when you select 128bits, you need to input 26 chars for HEX and 13 chars for ASCII.
Note	When the WPS is enabled, please not use WEP.

C. WPA-PSK

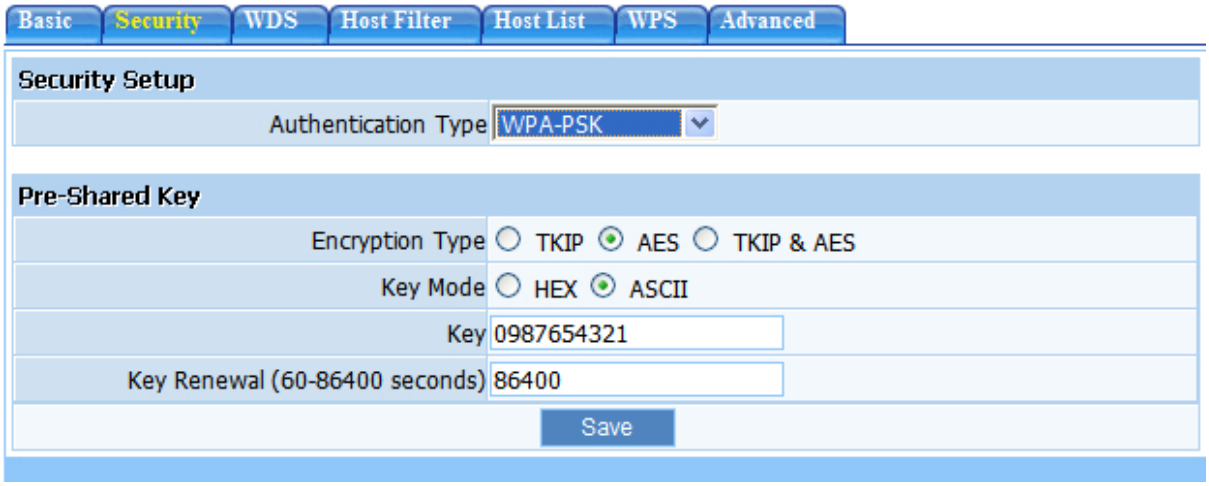


Figure 5-14 Security-WPA-PSK

The page includes the following fields:

Object	Description
Encryption type	You can select the algorithm you want to use, TKIP, AES or TKIP&AES. TKIP means "Temporal Key Integrity Protocol", which incorporates Message Integrity Code (MIC) to provide protection against hackers. AES, means "Advanced Encryption System", which utilizes a symmetric 128-Bit block data.
Key Renewal	you can configure the renewal time between 60 to 86400 seconds.
Key Length description	you need to input 8 to 63 ASCII characters no matter which type you select.

D. WPA2-PSK

The WPA2-PSK is similar to WPA-PSK and with stronger encryption method than WPA-PSK, using WPA2-PSK; you should input password (leave this value in the range of 8 to 63 characters) and key renewal time (leave this value in the range of 60 to 86400 seconds).

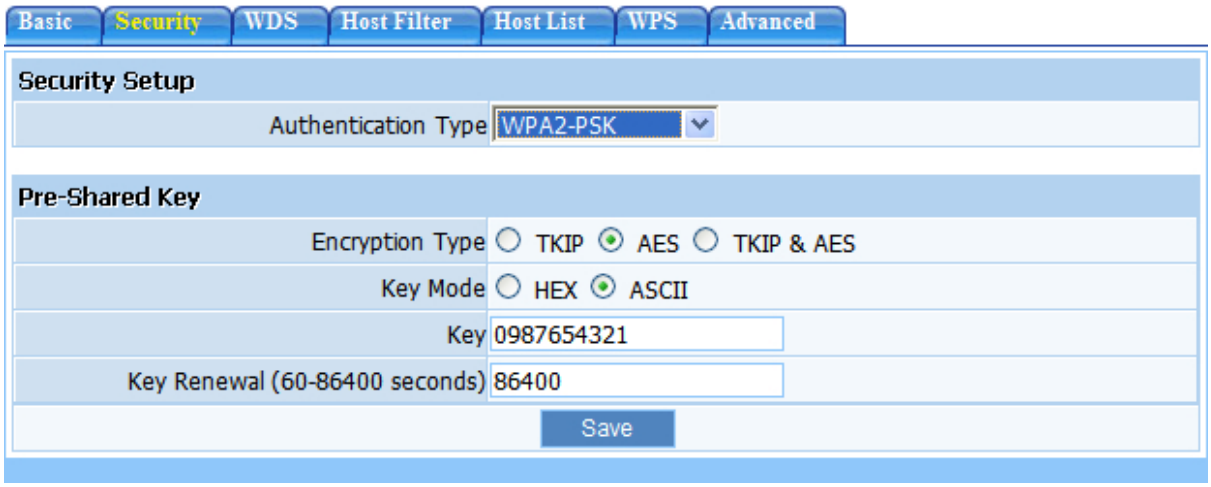


Figure 5-15 Security-WPA2-PSK

The page includes the following fields:

Object	Description
Encryption type	You can select the algorithm you want to use, TKIP, AES or TKIP&AES. TKIP means "Temporal Key Integrity Protocol", which incorporates Message Integrity Code (MIC) to provide protection against hackers. AES, means "Advanced Encryption System", which utilizes a symmetric 128-Bit block data.
Key Renewal	You can configure the renewal time between 60 to 86400 seconds.
Key Length description	You need to input 8 to 63 ASCII characters no matter which type you select.

E. WPA/WPA2-PSK

This item mixed WPA-PSK and WPA2-PSK mode, which provides higher security level; you can configure it according with WPA-PSK or WPA2-PSK.

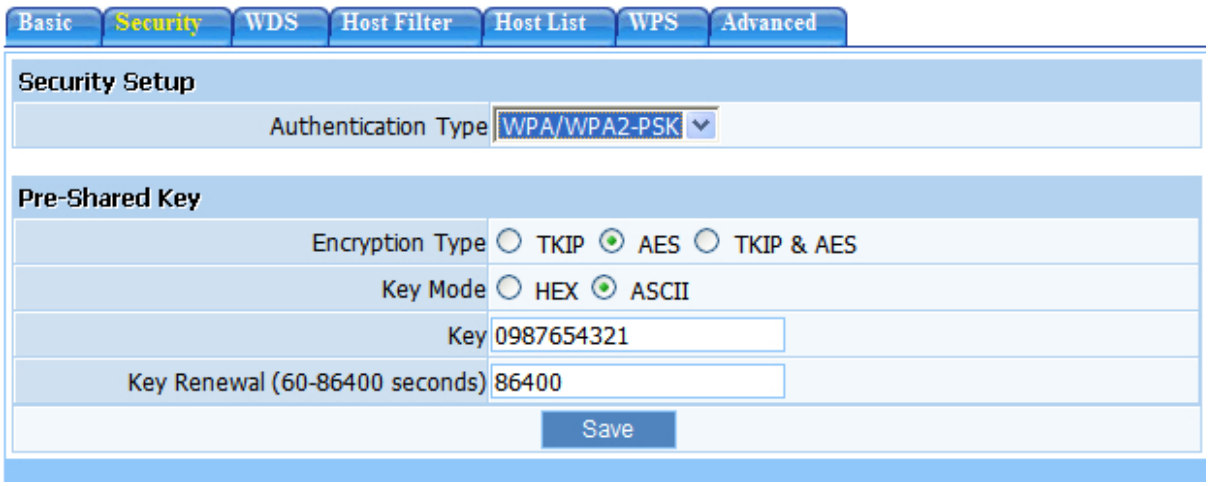


Figure 5-16 Security-WPA/WPA2-PSK

The page includes the following fields:

Object	Description
Encryption type	You can select the algorithm you want to use, TKIP, AES or TKIP&AES. TKIP means "Temporal Key Integrity Protocol", which incorporates Message Integrity Code (MIC) to provide protection against hackers. AES, means "Advanced Encryption System", which utilizes a symmetric 128-Bit block data.
Key Renewal	you can configure the renewal time between 60 to 86400 seconds.
Key Length description	you need to input 8 to 63 ASCII characters no matter which type you select.

5.4.1.3 WDS

If you have selected WDS or AP+WDS mode in Wireless Basic Radio Mode, please do the following configurations.

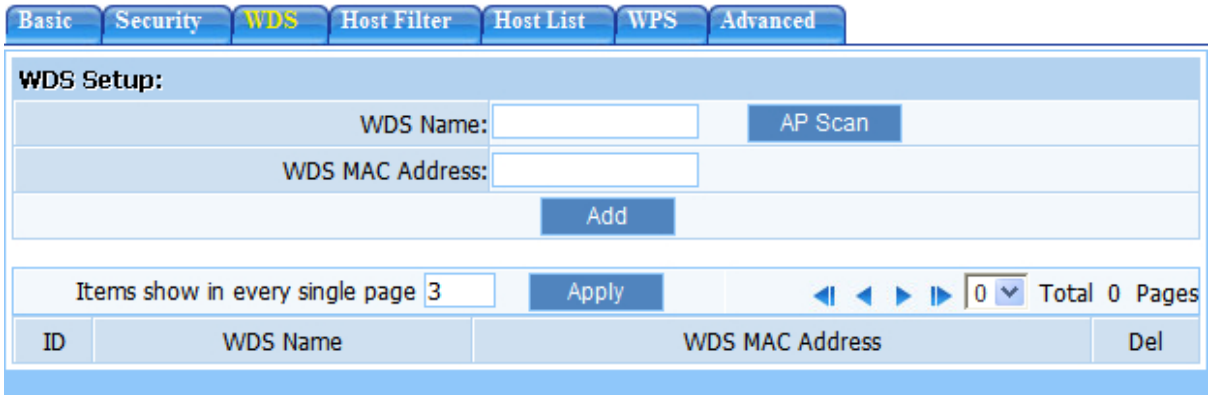


Figure 5-17 WDS

The page includes the following fields:

Object	Description
WDS Name	Give a description of your wireless bridge to tell apart.
WDS MAC Address	If the current working mode is "**WDS**" or "**AP+WDS**", then you need to configure wireless bridge configuration. Enter MAC address of remote access point, at the same time the remote access point also need to configure to "**WDS**" or "**AP+WDS**" mode.
Current WDS Information	It illustrates basic information of all wireless bridge that in connection status, you may delete unnecessary bridge.

5.4.1.4 Host Filter

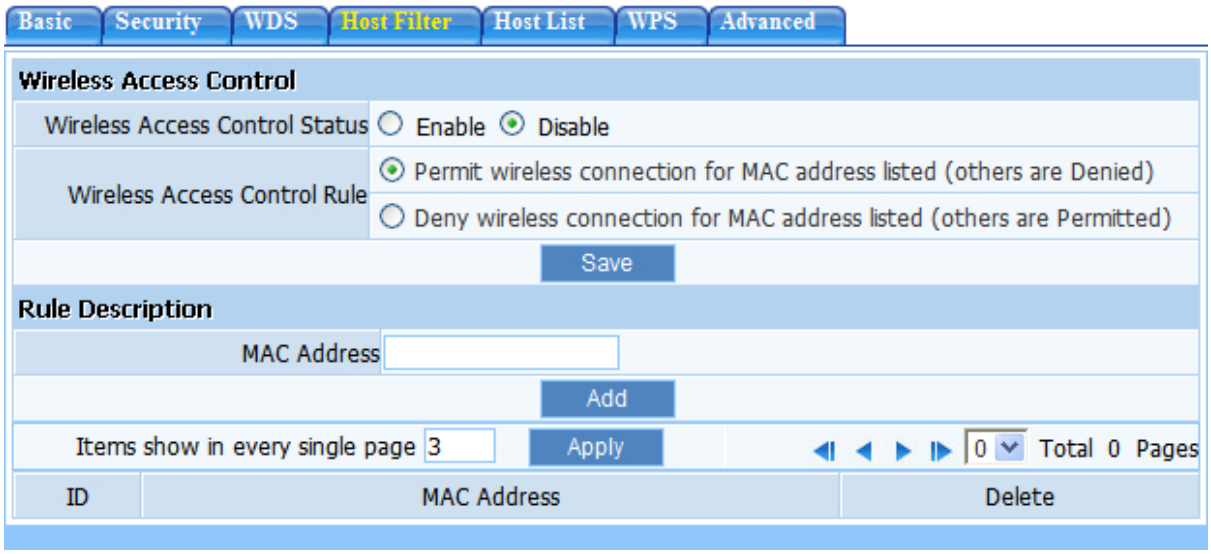


Figure 5-18 Host Filter

The page includes the following fields:

Object	Description
Wireless Access Control Status	The default is "**Disable**". You can filter wireless users by enabling this function; thus unauthorized users can not access the network.
Wireless Access Control Rule	You can select permit or deny. The default is permit.
MAC address	Input the MAC address that you want to control. The default format is XX:XX:XX:XX:XX:XX（e.g.: 00:30:4F:11:22:33）.

5.4.1.5 Host List

All this shows the current wireless access point by access to the state of the wireless station, easy to manage.

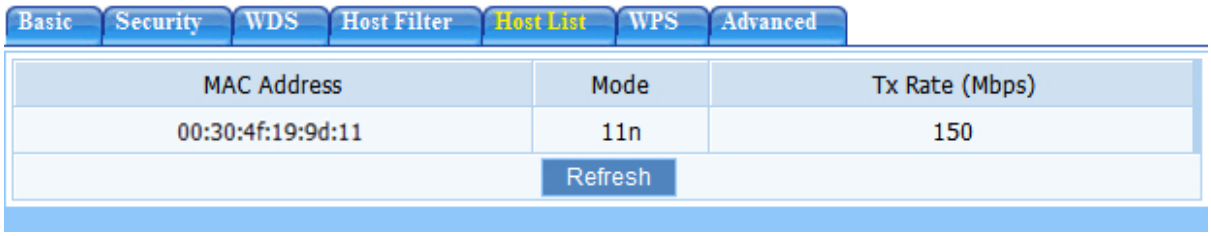


Figure 5-19 Host List

5.4.1.6 WPS

Wi-Fi Protect Setup (WPS) function can let you create a safety network easily. You can through "PIN Input Config (PIN)" to encrypt your network.

Note:

If you have configured encryption mode in your AP, then when you use this WPS function, please configure the authentication type to none, and then it will be encrypted to WPA2-AES mode automatically. If you don't want to change your authentication type, then when you use this function, the AP will be encrypted to the mode that you have configured.

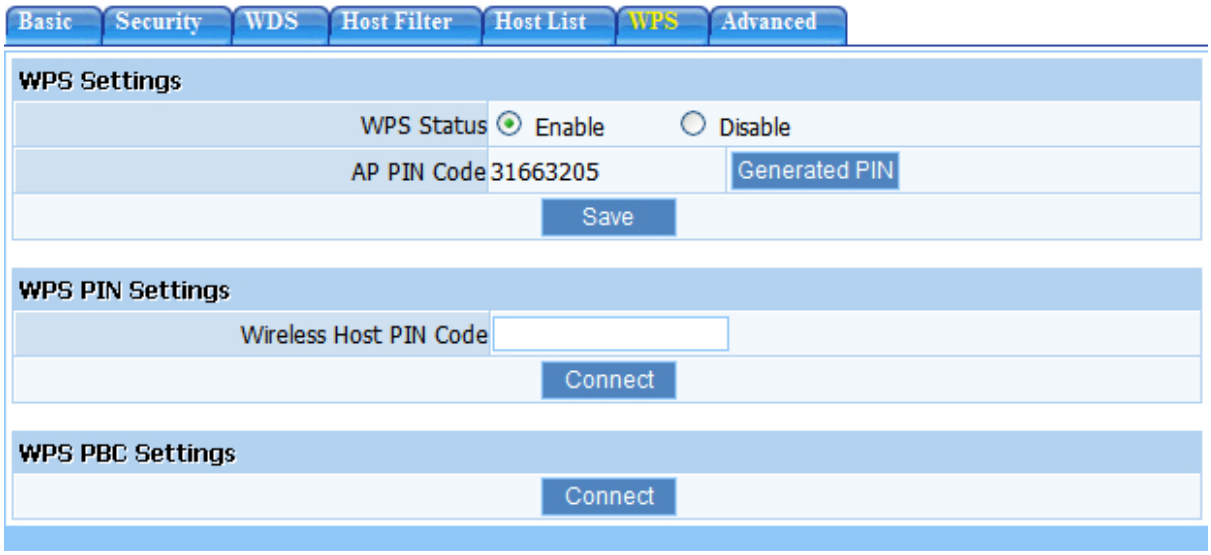


Figure 5-20 WPS

The page includes the following fields:

Object	Description
WPS Status	The default is "**Disable**". You can use this function to setup the wireless connection between this AP and wireless network card.
AP PIN Code	Here shows the AP's PIN code (Personal Identification Number) that the enrollee should enter the registrar's PIN code to make a connection. Click "**Generate PIN**" button to generate a new AP PIN code.
Wireless Host PIN Code	Input the PIN of wireless network card that support WPS function. Click "**Connect**", when it connect successfully, it will be encrypted to WPA2-PSK,
WPS PBC settings	Click "**Connect**", when it connect successfully, it will be encrypted to WPA2-PSK

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and AP using either Push Button Configuration (PBC) method or PIN method.

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

You may set up a safe network via the following methods:

I. By Push Button Configuration (PBC)

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Step 1: Choose WPS PBC Settings, and click "**Connect**".

Figure 5-21 WPS PBC Settings

Step 2: Press and hold the WPS Button equipped on the adapter directly for 2 or 3 seconds. Or you can click the WPS button with the same function in the configuration utility of the adapter.

Note

1) Step 1 & 2 should process within two minutes.

2) WNAP-6306 only supported Software PBC.

Step 3: Wait for a while until the connection established to complete the WPS configuration.

II. By PIN

If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN of your Wireless adapter into the configuration utility of the AP

Step 1: Choose WPS PIN Settings, and enter the PIN code of the wireless adapter.

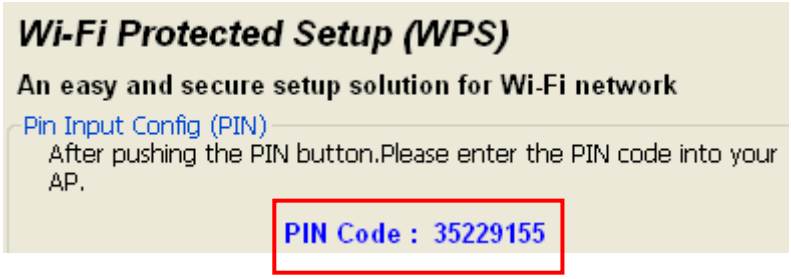


Figure 5-22 PIN of Wireless Adapter

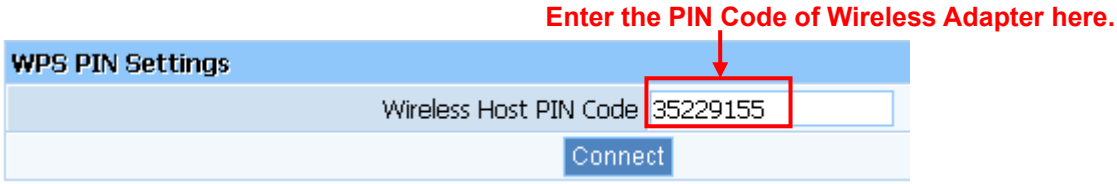


Figure 5-23 WPS PIN Settings

Note

The PIN code of the adapter is always displayed on the WPS configuration screen.

Step 2: For the configuration of the wireless adapter, please choose the option that you want to **enter PIN into the AP** in the configuration utility of the WPS, and click **Next.**

Method Two: Enter the PIN of the AP into the configuration utility of your Wireless adapter

Step 1: Choose PIN option, and get the Current PIN code of the AP in WPS Settings (each AP has its unique PIN code).

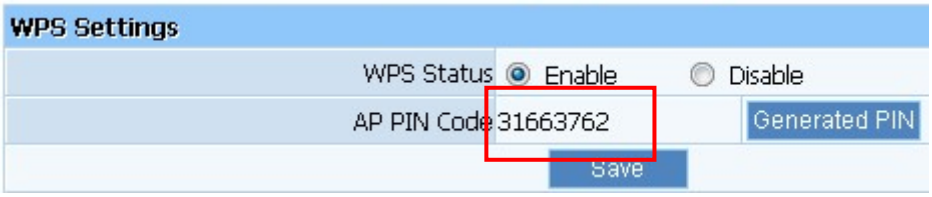


Figure 5-24 WPS – PIN of AP

Step 2: For the configuration of the wireless adapter, please choose the option that you want to **enter the PIN of the AP** in the configuration utility of the Wireless adapter, and enter it into the field. Then click **Next** to establish the connection.

Note

The WPS function cannot be configured if the Wireless Function of the AP is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

5.4.1.7 Advanced

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the change will have on your AP.

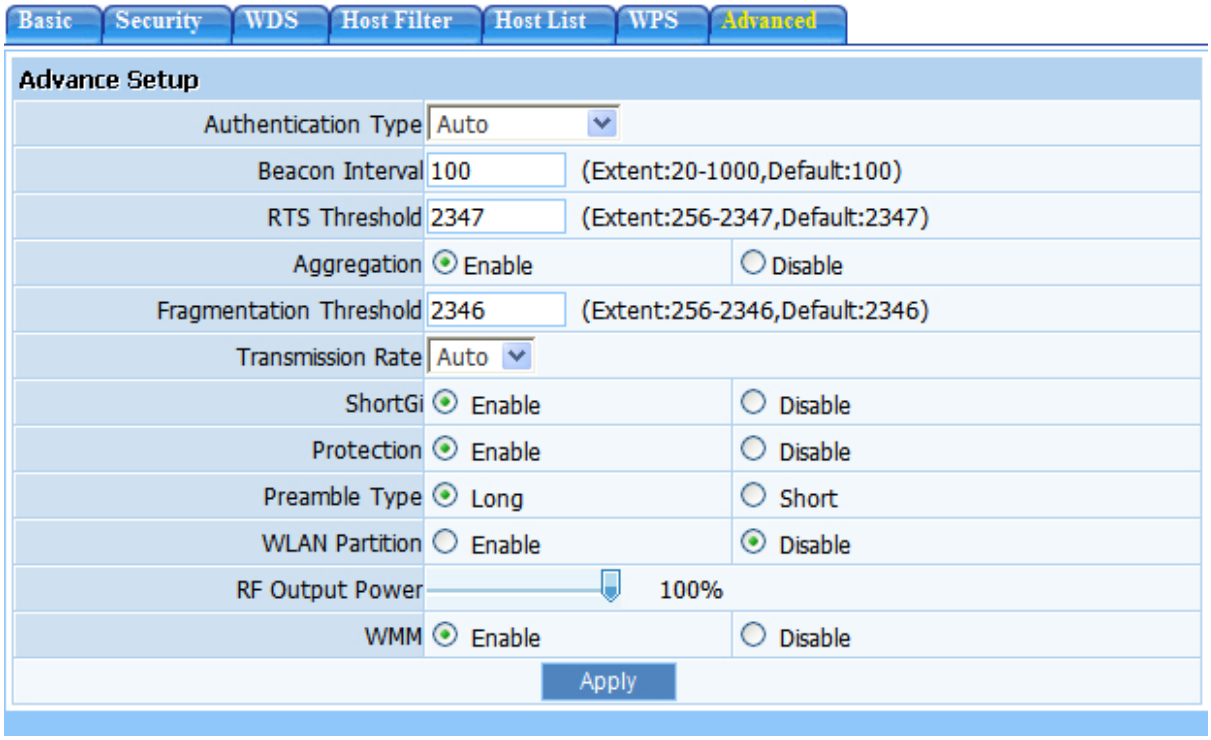


Figure 5-25 Advance Setup

The page includes the following fields:

Object	Description
Authentications type	The default is set to "**Auto**", which allows "Open System" or "Shared Key" authentication to be used. Select "Shared Key" if you only want to use "Shared Key" authentication (the sender and recipient use a WEP key for authentication).
Beacon Interval	Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). Beacon is used to synchronize the wireless network. The valid interval is 20-1000, the default is 100.
RTS Threshold	You can set RTS Threshold value in this field, the valid range should be 256-2347 and default value is 2347. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled.
Aggregation	You can accelerate the wireless transmission speed by enabling the aggregation function. The default is AMPDU+AMSDU.
Fragmentation Threshold	It specifies the maximum size of packet during the fragmentation of data to be transmitted.

Transmission Rate	Transmit rate indicates the transmission speed of wireless LAN access .The default setting is "**Auto**" and you can set this value between 1-150Mbps range.
ShortGi	You can select "**Enable**" or "**Disable**" for shortgi. It is used to set the time that the receiver waits for RF reflections to settle out before sampling data.
Protection	Using 802.11b and 802.11g mixed mode may result in poor network performance. By enabling 802.11 protection, it will ameliorate performance of 802.11g devices in your wireless network.
Preamble Type	"**Short Preamble**" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability; the default setting is "Long Preamble".
WLAN Partition	This feature is to isolate the communication of wireless clients connected with different AP. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other.
RF Output Power	Set the wireless output power level. The default value is 100%.
WMM	To enhance wireless multimedia transfer performance (0n-line video and voice).

5.4.2 Multiple AP Setup

The wireless AP supports multiple AP, if you need to open more than one AP, you can choose to open vice AP function. The default status of secondary AP is disabled; you can select enable to enable the secondary AP. Please refer to "**Wireless Setup Basic**" and "**Wireless Security**" for details.

5.4.2.1 Basic

The default status of secondary AP is disable, you can select enable to enable the secondary AP. Please refer to **5.3.1.1 Wireless Basic** for details

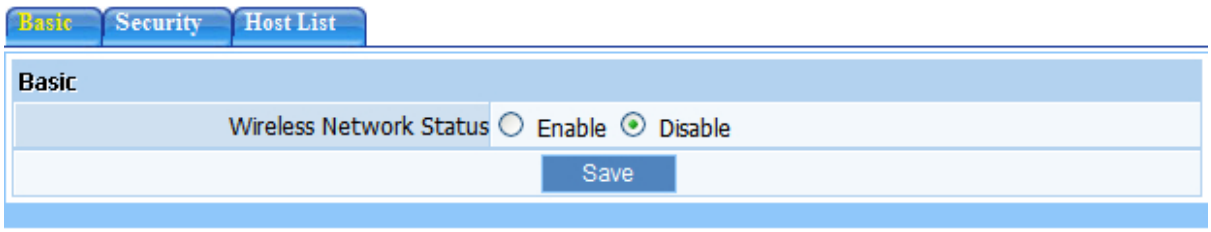


Figure 5-26 Multiple AP Setup – Basic

5.4.2.2 Security

Please refer to **5.3.1.2 Security** for details.

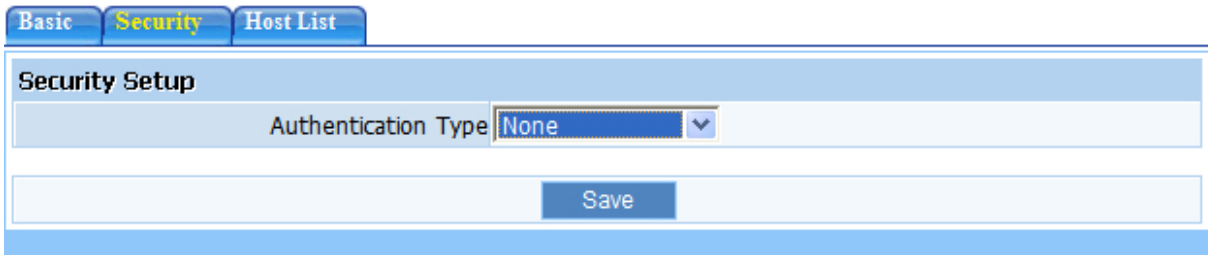


Figure 5-27 Multiple AP Setup - Security

5.4.2.3 Host List

Display current status of the wireless client associate with the secondary AP.

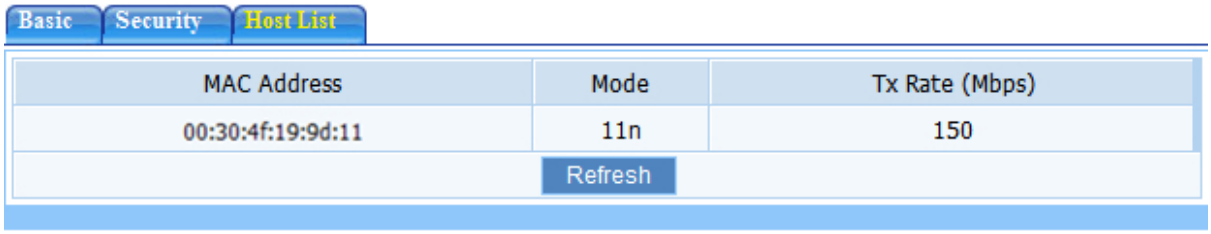


Figure 5-28 Multiple AP Setup - Host List

5.5 Wireless LED Thresholds

Please set the AP to the external LED lights and wireless signal strength received correspondence, when the AP receives the wireless signal, according to the wireless signal strength, the corresponding LED will be lit.

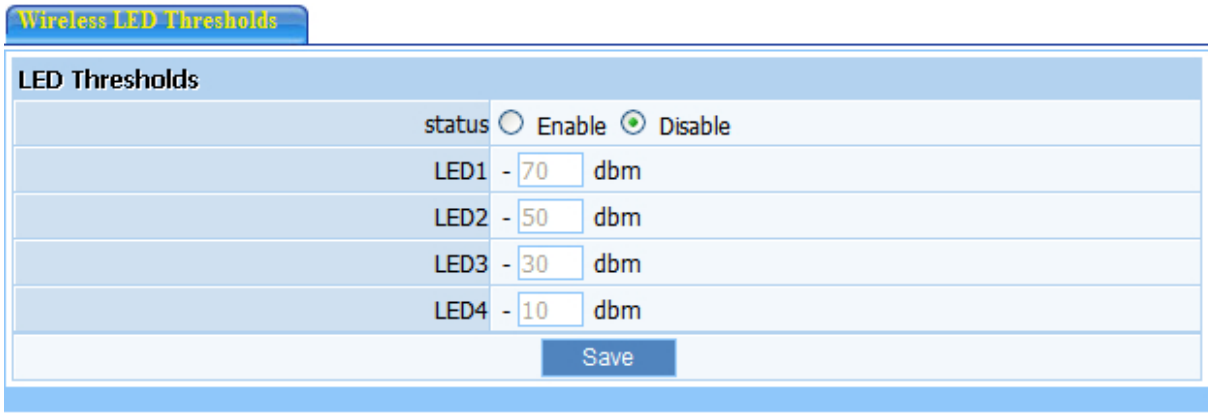


Figure 5-29 Wireless LED Thresholds

The page includes the following fields:

Object	Description
LED1	The LED1 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -70dBm.
LED2	The LED2 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -50dBm.
LED3	The LED3 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -30dBm.
LED4	The LED4 will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -10dBm.

5.6 LAN Setup

According to actual needs, you can choose on or off the DHCP server, and also modify the DHCP address pool range.

5.6.1 LAN IP Address

The IP address of LAN port is used for access AP itself by computers that connect to the AP directly; here you can set IP address you need. The IP address format is like XXX.XXX.XXX.XXX, and default IP address is **192.168.1.1**, the default subnet mask is **255.255.255.0**.

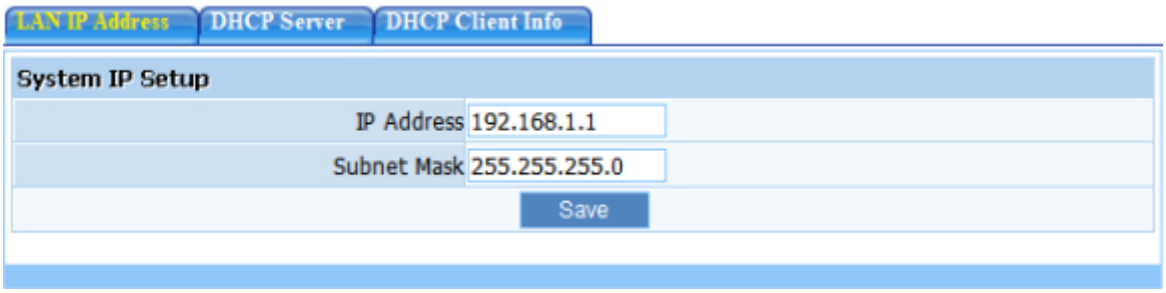


Figure 5-30 LAN IP Address

5.6.2 DHCP Server

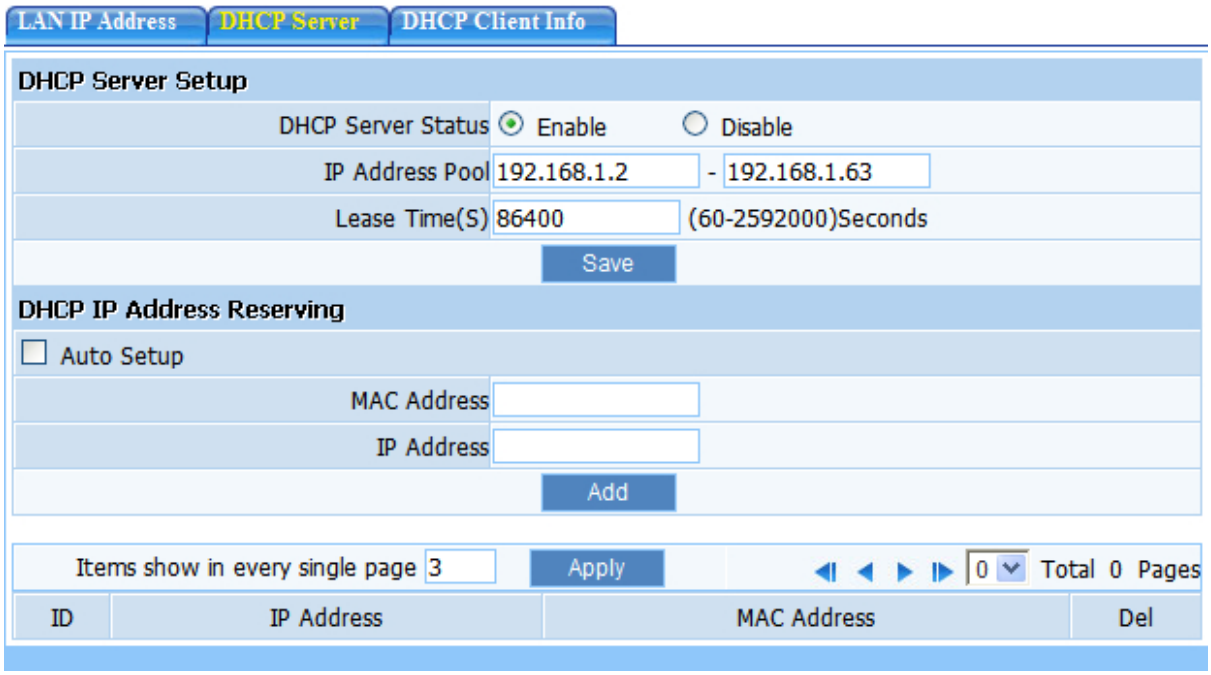


Figure 5-31 DHCP Server

The page includes the following fields:

Object	Description
DHCP Server Status	Keeps the default setting "**Enable**", so AP is able to use DHCP function. If a DHCP server has already existed in the network, please select "**Disable**".
IP Address Pool	The IP Address pool is used for allocate IP address by DHCP server; The IP Address pool range is also changeable
DHCP IP Address Reserving	Reserve IP address for designed physical address host. If you want to configure a fixed IP address for some host, please input physical address and IP address, then click add

5.6.3 DHCP Client Info

Display the state of assigned IP by DHCP Server

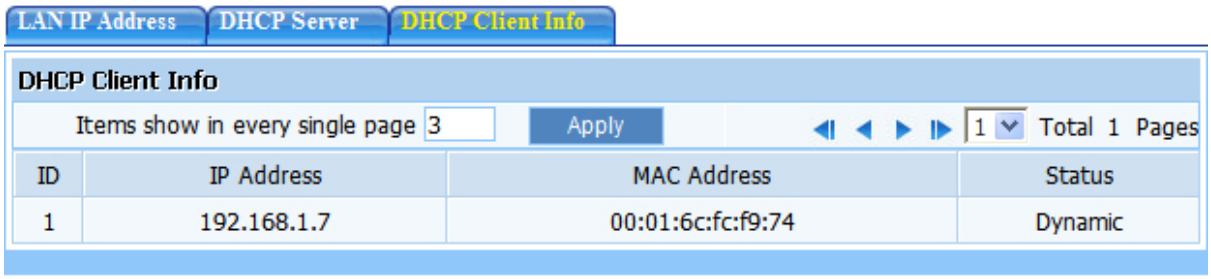


Figure 5-32 DHCP Client Info

5.7 Application & Game - UPnP

The UPnP function supports load Application's port forward record automatically. Select "**Enable**" to enable this function.

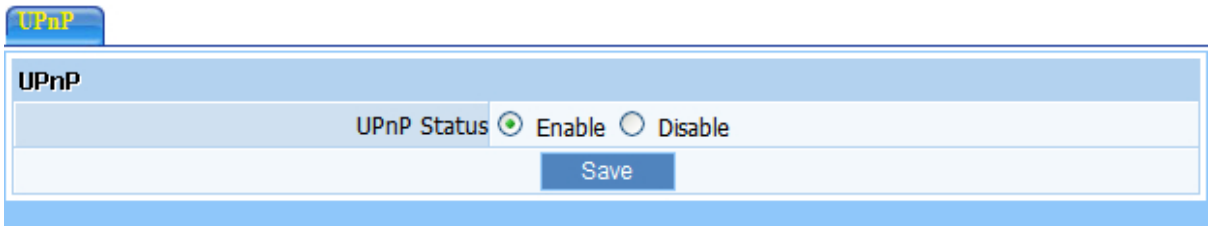


Figure 5-33 UPnP

5.8 Routing

Most of AP and wireless AP are using NAT mode, so this feature is designed for most common network environment. You can check out all current route items, click "**delete**" button to delete a route item existed in routing table.

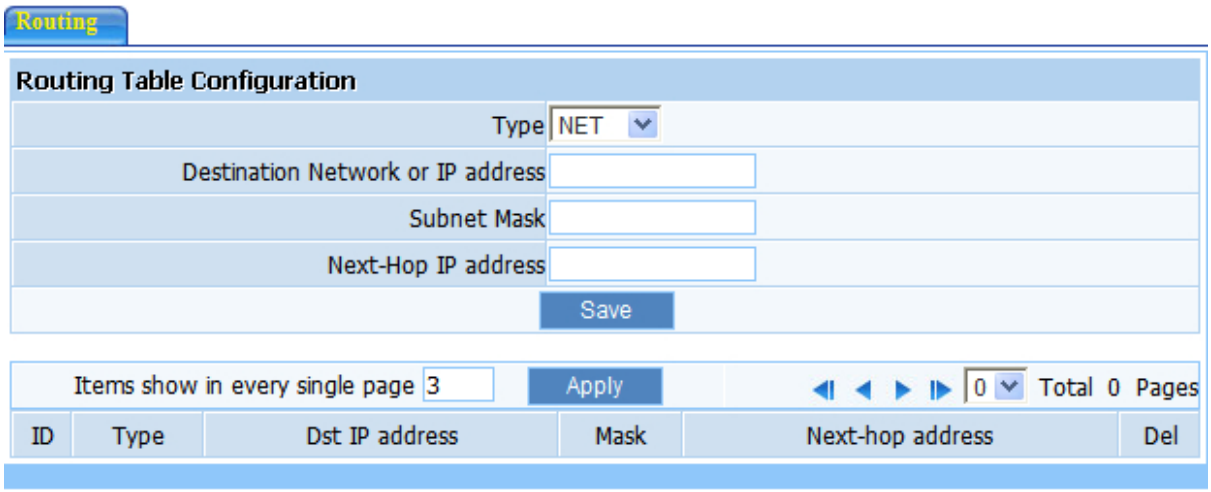


Figure 5-34 Routing

The page includes the following fields:

Object	Description
Type	Select "**NET**" Indicates that the Destination parameter should be interpreted as a network. Select "**HOST**" Indicates that the Destination parameter should be interpreted as a host.
Destination Network or IP Address	Specify a certain destination Network or IP address which static route forward to.
Subnet Mask	Subnet mask is used for distinguish Network portion and Host portion for an IP address.
Next-hop IP Address	This is an IP address of the next-hop device (and also is the gateway address for local host) that allows forwarding data between AP and remote network or host.

5.9 System Management

System management includes password setup, upgrade, reboot, backup, restore, WOL and System time.

5.9.1 Password Setup

The default username & password are both "**admin**". To ensure the AP's security, it is suggested that you change the default password to one of your choice, here enter a new password and then re-enter it again to confirm your new password. Click "**Save**" button to save settings.

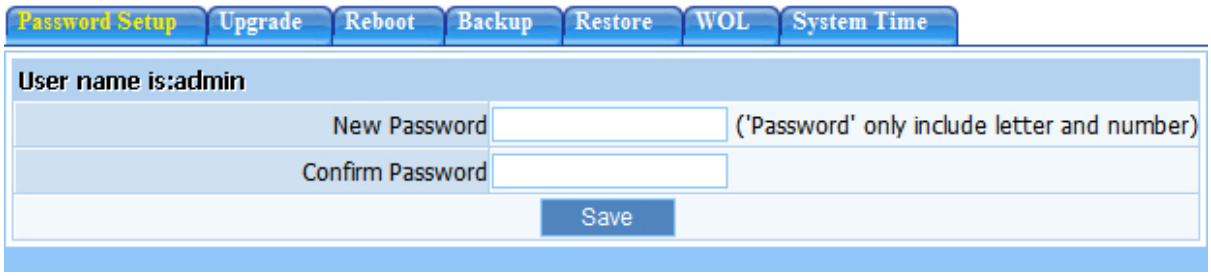


Figure 5-35 Password Setup

5.9.2 Upgrade

Click "**Upgrade**" and select a file to upgrade, after you have selected the appropriate file, click "**Upgrade**" button to execute upgrade procedure. Do not cut off the power supply during the process of upgrading.

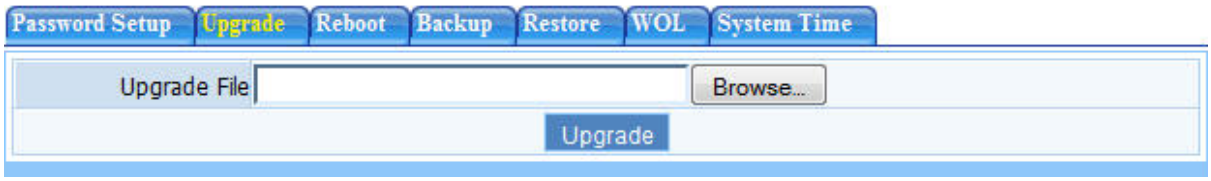


Figure 5-36 Upgrade

5.9.3 Reboot

Click "**Restart**" button to restart the AP.

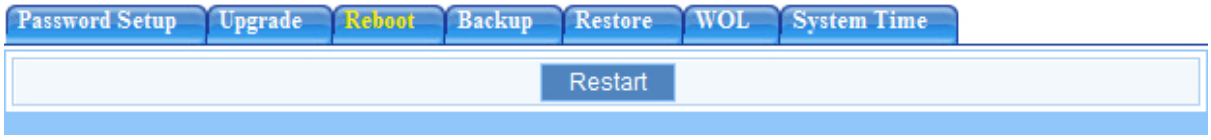


Figure 5-37 Reboot

5.9.4 Backup

Click "**Backup Parameter**" button to backup the system configuration, and click "**Parameter Recovery**" to restore the system configuration.

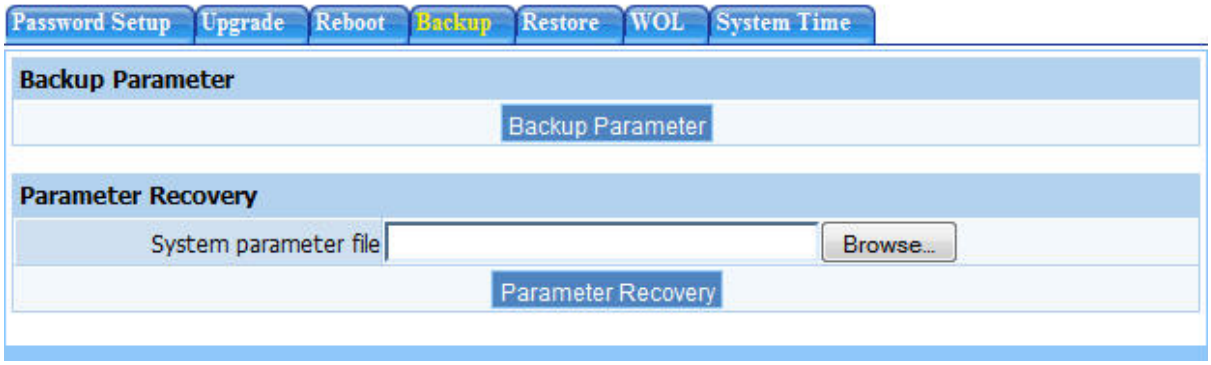


Figure 5-38 Backup

The page includes the following fields:

Object	Description
Backup Parameter	Click **Backup Parameter** button to export the current configuration to your PC.
Parameter Recovery	Click **Browse** button to select the configuration file from your PC, then click **Parameter Recovery** button to update the configuration.

5.9.5 Restore

Click "**Restore**" button, the AP will erase all of your settings and replace them with the factory defaults, make sure you have backup current settings before click this button.

Figure 5-39 Restore

5.9.6 WOL

Input host MAC address, and then click button of "**Wake up**" to wake up the target host which in the LAN.

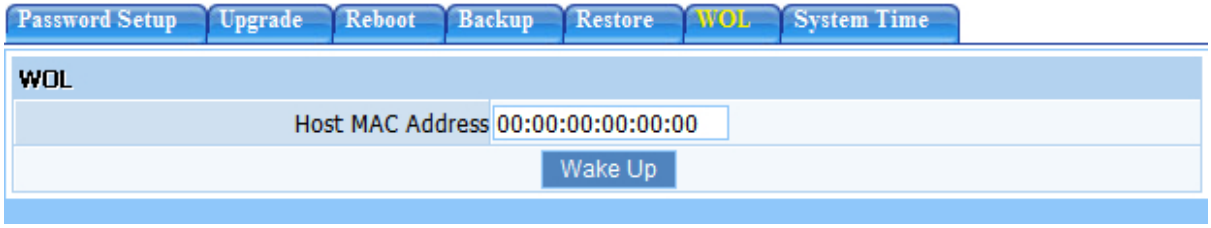


Figure 5-40 WOL

5.9.7 System Time

You can choose the time zone for the system time.

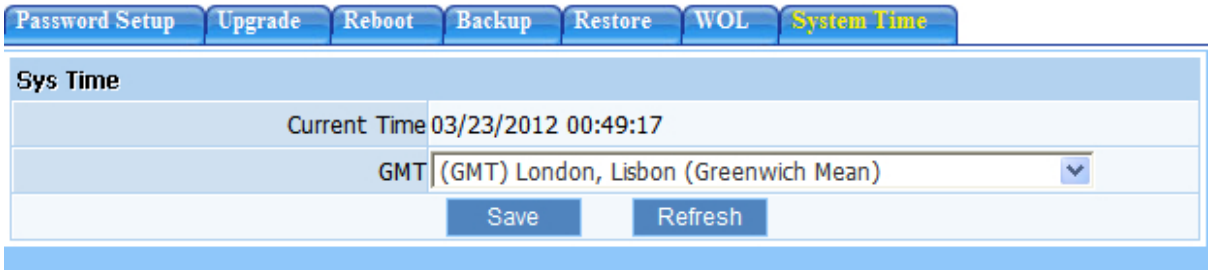


Figure 5-41 System Time

Appendix A: FAQ

1. What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

(1) Open the Command program in the Microsoft Windows.

(2) Type in "ipconfig /all", then press the Enter button.

(3) Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

2. What is Wireless LAN?

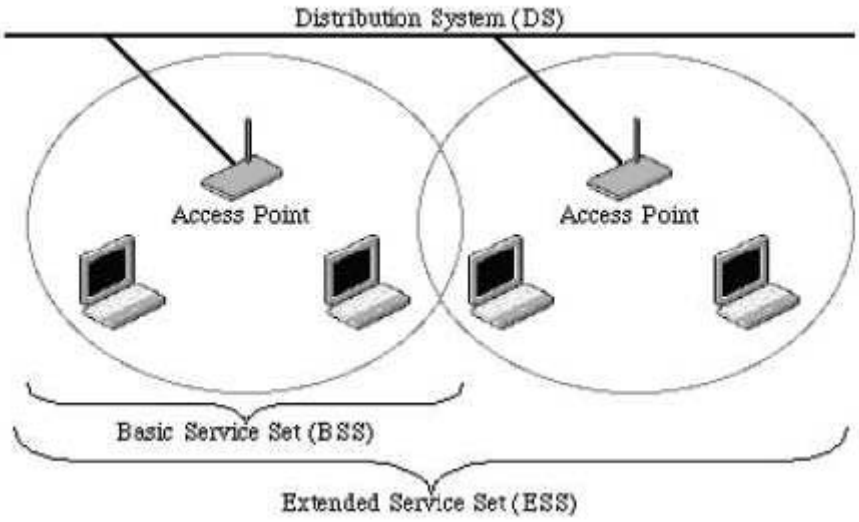
A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

3. What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/-13 MHz, 2450 +/-50 MHz and 5800 +/-75 MHz.

4. How does wireless networking work?

The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single sub-network. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).

Example 2: wireless Ad Hoc Mode

5. What is BSSID?

A six-byte address is that distinguish a particular a particular access point from others. Also know as just SSID. Serve as a network ID or name.

6. What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

7. What are potential factors that may causes interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture… etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- Minimizing the number of walls and ceilings.
- Position the WLAN antenna for best reception.
- Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors…etc.
- Add additional WLAN Access Points if necessary.

8. What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

9. What is WEP?

An option of IEEE 802.11 function is that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

10. What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead. Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.
If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

11. What is RTS (Request to Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/ CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

12. What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 include management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

13. What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

14. What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

15. What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

16. What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

17. What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

18. What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

19. What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

20. What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access

Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

21. What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless WDS or repeater service.

22. What is Universal Plug and Play (UPnP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

23. What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU.

24. What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address. Since that all the clients will communicate outside world through the WLAN Broadband Router, so have the cloned MAC address set on the WLAN Broadband Router will solve the issue.

25. What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user owned the DNS server with dynamic WAN IP address.

26. What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

27. What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to point private link via shared or public network.

28. What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

29. What is WLAN Block Relay between Clients?

An Infrastructure Basic Service Set is a BSS with a component called an Access Point (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS.

30. What is WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

31. What is WLAN ACK TIMEOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

32. What is Modulation Coding Scheme (MCS)?

MCS is Wireless link data rate for 802.11n. The throughput/range performance of an AP will depend on its implementation of coding schemes. MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream. Radios establishing and maintaining a link must automatically negotiate the optimum MCS based on channel conditions and then continuously adjust the selection of MCS as conditions change due to interference, motion, fading, and other events.

33. What is Frame Aggregation?

Every 802.11 packet, no matter how small, has a fixed amount of overhead associated with it. Frame Aggregation combines multiple smaller packets together to form one larger packet. The larger packet can be sent without the overhead of the individual packets. This technique helps improve the efficiency of the 802.11n radio allowing more end user data to be sent in a given time.

34. What is Guard Intervals (GI)?

A GI is a period of time between symbol transmission that allows reflections (from multipath) from the previous data transmission to settle before transmitting a new symbol. The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive.

Appendix B: Troubleshooting

1. I cannot access the Web UI from the Ethernet computer used to configure the AP.

- Check that the LAN LED is on. If the LED is not on, verify that the cable for the LAN connection is firmly connected.
- Check whether the computer resides on the same subnet with the AP's LAN IP address.
- If the computer acts as a DHCP client, check whether the computer has been assigned an IP address from the DHCP server. If not, you will need to renew the IP address.
- Use the ping command to ping the AP's LAN IP address to verify the connection.
- Make sure your browser is not configured to use a proxy server.
- Check that the IP address you entered is correct. If the AP's LAN IP address has been changed, you should enter the reassigned IP address instead.

2. I forget Password (Reset the AP without Login)

- Use a paper clip to press and hold the Default button on the back panel of the AP when it is working, wait for a few seconds until the SYS LED indicator stays green.
- After the above those steps, the manufacture's parameters will be restored in the AP. The default password is guest.

3. My wireless client cannot communicate with another Ethernet computer.

- Ensure the wireless adapter functions properly. You may open the Device Manager in Windows to see if the adapter is properly installed.
- Make sure the wireless client uses the same SSID and security settings (if enabled) as the Wireless AP
- Ensure that the wireless adapter's TCP/IP settings are correct as required by your network administrator.
- If you are using a 802.11b wireless adapter, and check that the 802.11G Mode item in Wireless Basic Setting page, is not configured to use 802.11G Performance.
- Use the ping command to verify that the wireless client is able to communicate with the AP's LAN port and with the remote computer. If the wireless client can successfully ping the AP' s LAN port but fails to ping the remote computer, then verify the TCP/IP settings of the remote computer.

Appendix C: Specifications

Product	**WNAP-6306** 150Mbps 802.11n Wireless Outdoor Access Point
Hardware Specification	
Standard support	IEEE802.11b/g IEEE 802.11n IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3x Flow Control
Memory	16 Mbytes DDR SDRAM 4 Mbytes Flash
Interface	Wireless IEEE802.11b/g/n LAN: 1 x 10/100Base-TX, Auto-MDI/MDIX
Antenna	Built-in N-Type (N-Male) Antenna Connector
Enclosure	IP65 waterproof case
PoE	Passive PoE 15~18V DC LAN RJ-45 Pin Assignment: PIN 4,5(+), PIN 7,8(-)
Wireless Interface Specification	
Frequency Band	2.4~2.4835GHz
Modulation	Transmission/Emission Type: DSSS / OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM, DBPSK, DQPSK, CCK
Data Rate	802.11b: 11, 5.5, 2 and 1 Mbps with auto-rate fall back 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6Mbps 802.11n (20MHz): up to 72Mbps 802.11n (40MHz): up to 150Mbp
Opt. Channel	America/ FCC: 2.414~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels) Japan/ TELEC: 2.412~2.484GHz (14 Channels)
Max. RF Output Power	802.11b: 20 ± 1dBm 802.11g: 19 ± 1dBm 802.11n: 16 ± 1dBm
Receiver Sensitivity	802.11b: -84dBm 802.11g: -68dBm 802.11n (20MHz): -65dBm 802.11n (40MHz): -62dBm
Media Access Control	CSMA/CA
Output Power Control	Range 1~100, default:100
Power Requirements	15~18V DC, 1A

Wireless Management Features	
Wireless Mode	■ AP ■ Client ■ WDS PtP ■ WDS PtMP ■ WDS Repeater (AP+WDS) ■ Universal Repeater (AP+Client)
Channel Width	20MHz / 40MHz
Encryption Security	64/128-bits WEP WPA, WPA-PSK WPA2, WPA2-PSK
AP Isolation/WLAN Partition	Enable it to isolate each connected wireless clients, to let them cannot access mutually.
Wireless Security	Wireless MAC address filtering
	Support WPS (WIFI Protected Setup)
	Enable/Disable SSID Broadcast
Multiple SSID	Support Dual-SSID
B/G Protection Mode	A protection mechanism prevents collisions among 802.11b/g modes
Association List	Display current status of the wireless client associate with AP
Max. Wireless Client	25
Max. WDS AP	4
Software	
LAN	Built-in DHCP server supporting static IP address distributing
	DHCP Reserve
Access Control	Support MAC filtering up to 20 MAC address
Max. Wired Client	60
Applications & Game	Support UPnP
Management	Web UI, DHCP Client, WOL
Diagnostic tool	System Log
Environment & Certification	
Operation Temp.	Temp.: -20~70°c, Humidity: 10%~95% non-condensing
Storage Temp.	Temp.: -30~80°c, Humidity: 5%~95% non-condensing
Regulatory	CE / RoHS

Appendix D: Glossary

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
CCK	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DDNS	Dynamic Domain Name Server
DH	Diffie-Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
MD5	Message Digest 5
NAT	Network Address Translation
NT	Network Termination
NTP	Network Time Protocol
PPTP	Point to Point Tunneling Protocol
PSD	Power Spectral Density
RF	Radio Frequency
SHA1	Secure Hash Algorithm
SNR	Signal to Noise Ratio
SSID	Service Set Identification
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UPNP	Universal Plug and Play
VPN	Virtual Private Network
WDS	Wireless Distribution System

WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

EC Declaration of Conformity

For the following equipment:

*Type of Product : 802.11n Wireless Outdoor Access Point

*Model Number : WNAP-6306

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.)

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 1999/5/EC R&TTE. For the evaluation regarding the R&TTE the following standards were applied:

EN 60950-1	(2006 + A11: 2009 + A1:2010)
EN 300 328 V1.7.1	(2006-10)
EN 301 489-1 V1.8.1	(2008-04)
EN 301 489-17 V2.1.1	(2009-05)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan *Place*

30th April, 2012 *Date*

Kent Kang *Legal Signature*

EC Declaration of Conformity

English	Hereby, **PLANET Technology Corporation,** declares that this **802.11n Wireless Outdoor AP** is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**Lietuviškai**	Šiuo **PLANET Technology Corporation,**, skelbia, kad **802.11n Wireless Outdoor AP** tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost **PLANET Technology Corporation,** tímto prohlašuje, že tato **802.11n Wireless Outdoor AP** splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	**Magyar**	A gyártó **PLANET Technology Corporation**, kijelenti, hogy ez a **802.11n Wireless Outdoor AP** megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation,** erklærer herved, at følgende udstyr **802.11n Wireless Outdoor AP** overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	**Malti**	Hawnhekk, **PLANET Technology Corporation,** jiddikjara li dan **802.11n Wireless Outdoor AP** jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt **PLANET Technology Corporation,** dass sich dieses Gerät **802.11n Wireless Outdoor AP** in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)	**Nederlands**	Hierbij verklaart , **PLANET Technology orporation,** dat **802.11n Wireless Outdoor AP** in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eesti keeles	Käesolevaga kinnitab **PLANET Technology Corporation,** et see **802.11n Wireless Outdoor AP** vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation,** oświadcza, że **802.11n Wireless Outdoor AP** spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 1999/5/EC".
Ελληνικά	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , **PLANET Technology Corporation,** *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* **802.11n Wireless Outdoor AP** *ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*	**Português**	**PLANET Technology Corporation,** declara que este **802.11n Wireless Outdoor AP** está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Español	Por medio de la presente, **PLANET Technology Corporation,** declara que **802.11n Wireless Outdoor AP** cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE	**Slovensky**	Výrobca **PLANET Technology Corporation,** týmto deklaruje, že táto **802.11n Wireless Outdoor AP** je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 1999/5/EC.
Français	Par la présente, **PLANET Technology Corporation,** déclare que les appareils du **802.11n Wireless Outdoor AP** sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**Slovensko**	**PLANET Technology Corporation**, s tem potrjuje, da je ta **802.11n Wireless Outdoor AP** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente , **PLANET Technology Corporation,** dichiara che questo **802.11n Wireless Outdoor AP** è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva. 1999/5/CE.	**Suomi**	**PLANET Technology Corporation,** vakuuttaa täten että **802.11n Wireless Outdoor AP** tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo **PLANET Technology Corporation,** apliecina, ka šī **802.11n Wireless Outdoor AP** atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation,** att denna **802.11n Wireless Outdoor AP** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.